Future Mode of Operations for 5G - The SELFNET Approach Enabled by SDN/NFV

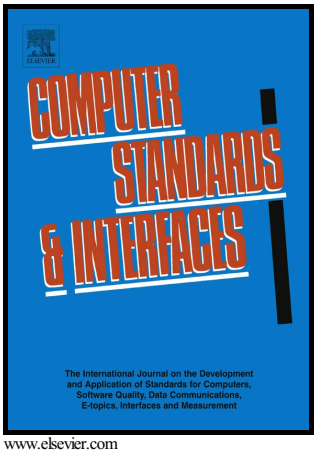
Neves, Pedro ; Calé, Rui ; Costa, Mário ; Gaspar, Gonçalo ; Wang, Qi; Alcaraz Calero, Jose M.; Nightingale, James; Bernini, Giacomo ; Carrozzo, Gino ; Valdivieso, Ángel ; Villalba, Luis Javier García ; Barros, Maria João ; Gravas, Anastasius ; Santos, José ; Maia, Ricardo ; Preto, Ricardo

Published in:
Computer Standards & Interfaces

DOI:
10.1016/j.csi.2016.12.008

E-pub ahead of print: 20/02/2017

Document Version
Peer reviewed version



Future Mode of Operations for 5G – The SELFNET Approach Enabled by SDN/NFV

Pedro Neves, Rui Calé, Mário Costa, Gonçalo Gaspar, Jose Alcaraz-Calero, Qi Wang, James Nightingale, Giacomo Bernini, Gino Carrozzo, Ángel Valdivieso, Luis Villalba, Maria Barros, Anastasius Gravas, José Santos, Ricardo Maia, Ricardo Preto

PII: S0920-5489(16)30243-4
DOI: http://dx.doi.org/10.1016/j.csi.2016.12.008
Reference: CSI3185

To appear in: *Computer Standards & Interfaces*

Received date: 18 April 2016
Revised date: 15 October 2016
Accepted date: 31 December 2016

Cite this article as: Pedro Neves, Rui Calé, Mário Costa, Gonçalo Gaspar, Jos Alcaraz-Calero, Qi Wang, James Nightingale, Giacomo Bernini, Gino Carrozzo Ángel Valdivieso, Luis Villalba, Maria Barros, Anastasius Gravas, José Santos, Ricardo Maia and Ricardo Preto, Future Mode of Operations for 5G – Th SELFNET Approach Enabled by SDN/NFV, *Computer Standards & Interfaces* http://dx.doi.org/10.1016/j.csi.2016.12.008

Future Mode of Operations for 5G – The SELFNET Approach Enabled by SDN/NFV

Pedro Neves[1], Rui Calé[1], Mário Costa[1], Gonçalo Gaspar[1], Jose Alcaraz-Calero[2], Qi Wang[2], James Nightingale[2], Giacomo Bernini[3], Gino Carrozzo[3], Ángel Valdivieso[4], Luis Villalba[4], Maria Barros[5], Anastasius Gravas[5], José Santos[6], Ricardo Maia[6], Ricardo Preto[7]

[1] Altice Labs, Rua Eng. José Ferreira Pinto Basto, 3810-106 Aveiro, Portugal

[2] University of the West of Scotland (UWS), High Street, Paisley PA1 2BE, United Kingdom

[3] Nextworks, via Livornese 1027, 56122, San Piero a Grado, Pisa, Italy

[4] Group of Analysis, Security and Systems (GASS), Faculty of Computer Science and Engineering, The Complutense University (UCM), Calle Profesor Jose Garcia Santesmases, 9, Ciudad Universitaria, 28040 Madrid (Spain)

[5] Eurescom, Wieblinger Weg 19, 69123 Heidelberg, Germany

[6] PROEF, Rua das Condominhas, 15/29 4150-222, Porto, Portugal

[7] Ubiwhere, Rua Pedro Vaz de Eça 6A, 3800-322 Aveiro, Portugal

pedro-m-neves@alticelabs.com[1], cale@alticelabs.com[1], mcosta@alticelabs.com[1], goncalo-n-gaspar@alticelabs.com[1], jose.alcaraz-calero@uws.ac.uk[2], qi.wang@uws.ac.uk[2], g.bernini@nextworks.it[3], g.carrozzo@nextworks.it[3], angevald@ucm.es[4], javiergv@fdi.ucm.es[4], gavras@eurescom.eu[5], barros@eurescom.de[5], josep.santos@proef.pt[6], ricardo.maia@proef.pt[7], rpreto@ubiwhere.com[7]

Abstract

The 5G infrastructure initiative in Europe[1] has agreed a number of challenging key performance indicators (KPIs) to significantly enhance the user experience and support a number of use cases with very demanding requirements on the network infrastructure. At the same time there is high pressure on the reduction of the operational expenditure (OPEX). A contribution to meeting the KPIs and to reduce OPEX is to evolve the management of the network into a fully autonomic and intelligent framework. Based on advanced technologies, such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV), the EU H2020 project SELFNET (https://selfnet-5g.eu/) is proposing an advanced network management framework to achieve these objectives.

Keywords

Network Functions Virtualization, Software Defined Networking, 5G, Self-Organizing Networks, Autonomic Management

1. Introduction

The European society and economy have recognized the strong dependency on a reliable, robust and widely available future network infrastructure. From its inception the new network infrastructure, called 5G infrastructure, should support a wide range of usage scenarios that can broadly be categorized in (i) Enhanced Mobile Broadband that addresses the human-centric use cases for access to multi-media content, services and data, including improved performance, wide-area coverage and seamless user experience; (ii) Ultra-reliable and low latency communications that is characterized by stringent requirements for capabilities such as throughput, latency and availability, and (iii) Massive machine type communications that is characterized by a very large number of connected devices typically transmitting a relatively low volume of non-delay sensitive data.

The European telecommunications industry and the European Commission have entered a Public-Private-Partnership (5G-PPP) to deliver solutions, architectures, technologies and standards for the ubiquitous next generation communication infrastructures of the coming decade. The future network infrastructure will help the transformation in several economic sectors, ranging from factories, automotive, e-health, energy, media & entertainment, and others.

Part of the "big picture" that guides the research and innovation activities in the 5G-PPP is Cognitive Network Management, with the ambition to develop a new management paradigm and investigate, develop and verify processes, algorithms and solutions that enable future 5G networks to be self-managed. The expected impacts of this work are (i) decreased OPEX by means of novel processes, architecture and functions, (ii) improved quality of service, user experience, dependability and security and (iii) consensus on future network management as a basis for standardization. In this context SELFNET concentrates on an autonomic network management framework for SDN/NFV-

[1] 5G Infrastructure Public Private Partnership, [Online]. Available here: https://5g-ppp.eu/

enabled 5G networks. Among others SELFNET defines the overall architecture, and designs and prototypes an automated physical and virtual infrastructure and network service deployment system, compliant with the 5G Mobile Edge Computing (MEC) paradigm. It designs and prototypes the mechanisms for the lifecycle and repository management of SDN and NFV apps as well as for the on-boarding and access to these apps, thereby paving the way for on-demand service deployment and operation. Furthermore SELFNET designs and prototypes the network monitoring facilities to gather performance metrics and events from the services and the physical/virtual infrastructures, enabling network management intelligence to obtain fast and improved decisions and take actions to assure service provisioning. Finally it prototypically demonstrates the capabilities of the framework via three representative use cases in self-healing against existing or predicted network/service failures, self-protection against network/service security threats especially distributed denial of services, and self-optimisation to maintain or improve Quality of Experience for video applications.

Section 2 of this paper describes the current network management paradigms and the problems associated with it, and outlines a vision for future network operations and management. Section 3 elaborates on the global standards that are relevant and suitable to support the implementation of the vision. The same section presents also a survey of the most important and promising open source initiatives that are candidates to become part of the implementation. Section 4 presents the core part of the work; namely the SELFNET reference architecture & Interfaces, which outlines the relevant system parts and the interrelationship among the parts, justifying certain design choices that have been made. Section 5 presents how the architecture supports the workflows of the use cases that are used for validation of the framework. Section 6 describes how existing and emerging standards and open source projects are being used in the context of the SELFNET architecture. Finally, Section 7 presents conclusions and future work.

2. Future Mode of Operations

This section describes the current paradigm for the services and network management, highlighting the existing limitations that telecom operators have to face on a daily basis (section 2.1). Furthermore, it also presents (section 2.2) the evolution towards an autonomic network management paradigm, based on network virtualization, network programmability and self-organizing concepts, in which the existing limitations are highly mitigated.

2.1. Traditional Network Management Paradigm

The current networking management paradigm, illustrated in Figure 1, poses a number of challenges to network operators. In particular, the management of anomalies and upgrades in the regular behaviour of the network are one of the main sources of increasing both capital and operational expenditures. Nowadays, operators have to do their best to detect and mitigate all sorts of problems in the networks such as link failures, performance bottlenecks, security attacks, QoS degradation, software bugs, and hardware faults, among others. Existing solutions typically require manual re-configuration of the equipment, and in some cases, the only solution is the deployment of new equipment and functionalities such as routers, NATs, firewalls, intrusion detection systems, load balancers, probes, etc. These tasks cannot be performed without affecting even for limited time the normal operation of the network. This causes disruptions in the services and violations in SLAs, thereby incurring in increased operational and capital costs and compromised end users' QoE.

Although this is a valid operation paradigm it is already somehow limited in the current network scenario so it will certainly not cope with the flexibility and dynamism required for the operation of NFV/SDN networks.

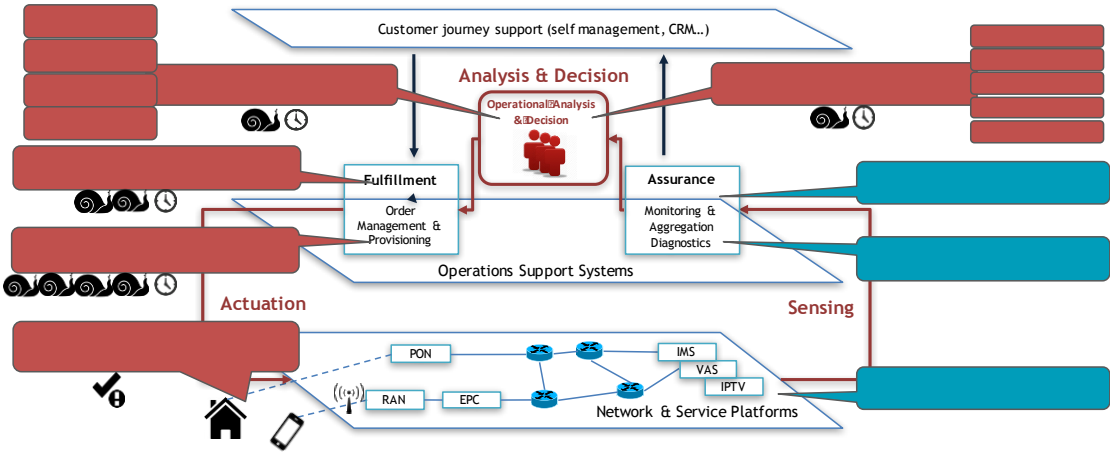


Figure 1: Traditional Network Management Paradigm

2.2. Evolving Towards an SDN/NFV-enabled Network Management Paradigm

Research in recent years in the area of SDN and NFV has resulted in the emergence of new capabilities that significantly improve the agility, flexibility and cost efficiency to manage network functions. These capabilities are the foundations to trigger a paradigm shift in the way network operations are planned and deployed, called autonomic management.

This new management approach will explore SDN, NFV and cloud computing technologies, together with novel algorithms, to achieve a highly intelligent paradigm for smart self-management of complex networking scenarios.

One of the main impacts of introducing autonomic capabilities is to significantly reduce the operational costs directly related to the management of the network. Essential network management tasks are automated, which will enable remarkable reduction in the complexity of the network management currently being manually conducted. Proactive and reactive actions are automated in order to resolve/mitigate networking problems, thereby minimizing the current labour-intensive maintenance and troubleshooting tasks for network operators, leading to more significant decrease in OPEX. This paradigm is illustrated in Figure 2.

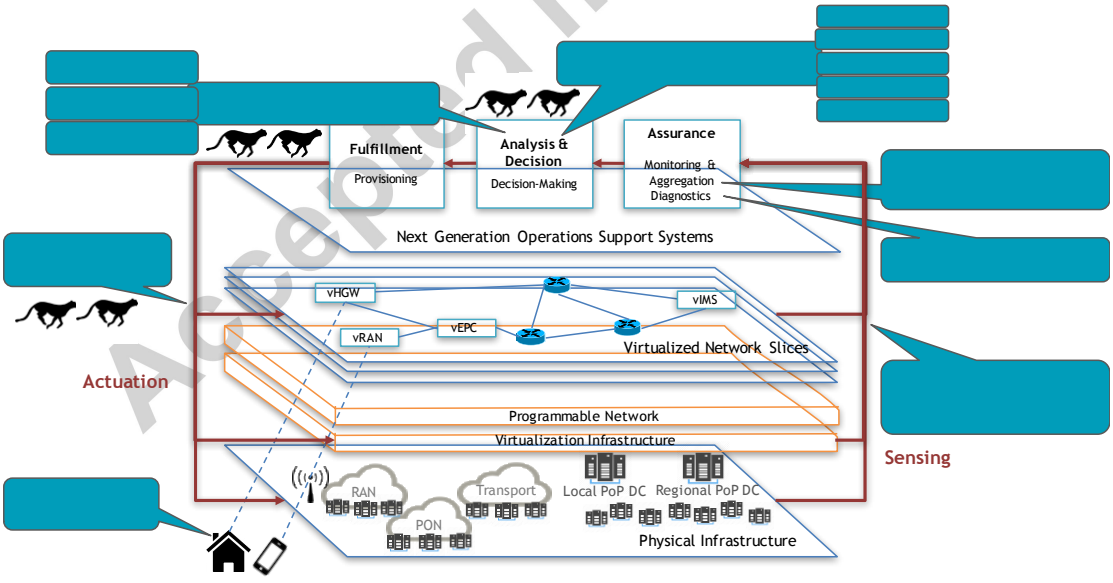


Figure 2: SDN/NFV-enabled Network Management Paradigm

In order to provide a fully-automated and highly intelligent autonomic management system, three key properties must be fulfilled by the architecture. The first one is related with **automated network monitoring.** The architecture should enable the automatic deployment of NFV applications in the network infrastructure, typically known as probes or sensors, to facilitate system-wide distributed monitoring. These virtual applications are spread across the access and backbone network

infrastructures to enable end-2-end user, service and network awareness through the collection of metrics from all required elements in the network architecture. The collected information must feed data analysis algorithms (e.g., data analytics, data mining, machine learning) in order to create key indicators that may translate to (1) service affecting conditions (network failures, performance bottlenecks, security braches, intrusions, etc., (2) conditions that may evolve to service affecting conditions in the future, (3) non optimal service delivery to specific users, i.e., detection of situations where the service topology being used to deliver a service to end users can be optimized in order to minimize the allocated resources or the service QoS. Packet inspection tools such as intrusion detection systems, selective packet processing tools, users profiling tools and network monitoring tools are some examples of software used to gather measurements to derive these high-level metrics.
The second key aspect that must be fulfilled by the new management architecture is the **autonomic network maintenance**, i.e., the ability to define high-level tactical corrective and preventive measures to respond to the diagnosed conditions. These tactical measures may correspond to reactive actions of the network with the aim to fix/mitigate existing network issues of various kinds, or may correspond to proactively actions to prevent the evolution of the diagnosed condition to an effective service affecting anomaly. These actions may be mapped to request for automated configuration, scalability, migration of existing VNF's, the deployment of new VNF's or the reconfiguration of services connectivity logical topology.
The combination of automated network monitoring with the automated network maintenance is the backbone of the autonomic service management, contributing to maximize the chances of sustaining the healthy operation of the network (and services), enabling intelligence-driven responses even in scenarios unknown a priori and without requiring human decisions and intervention.
Finally, the third key feature, is the **automated & dynamic service provisioning** taking into account not only the service type characteristics but also the status of the network architecture. This comprises dynamic smart selection of the best locations where the services should be deployed (or migrated to) considering the requirements associated with the specific service instance being provisioned (for instance the contracted QoS). It also includes the key indicators produced by the automated network monitoring that translate the network health (anomalies, performance), in order to guarantee that the provisioning of new services also contributes to maintaining the required levels of network performance, health and security.
The evolution towards an SDN/NFV-enabled network management paradigm is currently being addressed in the R&D SELFNET project [1] [2] [3] funded by the H2020 EU programme.

3. Relevant Standards & Open Source Projects Activities

This section provides a brief summary of all the standardization activities (section 3.1) and open source projects (section 3.2) that are relevant for the specification and implementation of an NFV/SDN-enabled autonomic network management framework.

3.1. Relevant Standardization Activities

3.1.1. ETSI NFV

The ETSI NFV Industry Specification Group (ISG) was created in 2012 by a number of network operators across the world to standardize the virtualization of network functions and define a complete architecture to accommodate the challenges of this new virtualization paradigm, covering both operational and management aspects. Table 1 shows the main activities of ETSI NFV.

Main Activities	Description
NFV architecture [4]	Design principles and the high-level functional decomposition of the ETSI NFV architecture. It identifies main components and interactions for VNFs and Network Services operation and management.
MANO architecture [5]	Management and orchestration framework required for the provisioning of VNFs and Network Services. Focuses on the definition of VNF and Network Service lifecycle management workflows, information elements and interfaces.
VNF architecture [6]	Identifies the most common and relevant software architectural patterns for VNFs implementation, including de-composition in individual software components.
SDN Usage in NFV Framework [7]	Common design patterns for using and integrating SDN in an NFV architectural framework.

Table 1: ETSI NFV Standardization Activities

The whole NFV paradigm, as presented in the ETSI NFV architecture specifications, is a key concept fully adopted in SELFNET to evolve the traditional network management towards highly flexible and programmable approaches where the combination of virtualized network functions (VNFs) and services enables agile self-organized behaviors for 5G services. Moreover, the SELFNET NFV Orchestration and Management Layer described in section 4.1 is aligned with the ETSI NFV MANO principles, functional decomposition and interfaces defined for lifecycle management and operation of VNFs and Network Services. In particular, ETSI NFV MANO components (mainly NFV Orchestrator and VNF Manager) and interfaces are adopted in SELFNET and enhanced (as detailed in Table 10) in support of hybrid orchestration of legacy, virtualized and programmable network functions and services. This allows network operators to apply a smooth transition to the aforementioned new management paradigm, where legacy services and management functions are gradually augmented with SDN and NFV capabilities.

However, SELFNET does not limit its engagement with the ETSI NFV ISG to the adoption of standard architectures and interfaces. Indeed, SELFNET is pushing its hybrid orchestration approach in the ETSI NFV community with the aim of providing concrete contributions to evolve the current status of the standards. With this respect, concrete inputs have been already provided to the ETSI NFV Security group (with positive feedback) for integration of the SELFNET self-protection capabilities (as described in section 5.2) into the NFV standard tracks.

3.1.2. ONF

Open Networking Foundation (ONF) [8] is a non-profit organization with over 100 members (services providers, network operators and private companies) that promote the adoption of SDN in the industry and research community. Table 2 shows the main activities of ONF.

Main Activities [9]	Description
SDN Reference Architecture	Defines the SDN architecture and interfaces of three layers: 1) Data Layer (physical network devices), ii) Control Layer (SDN Controller) and iii) Application Layer, and two interfaces to connect these layers.
Open Datapath	Defines the components and functions of the OpenFlow Switch, which is managed by an external entity known as the Controller. It is able to change (add, update, delete) the flow entries in a flow table through a secure channel. The SBI used for this communication is OpenFlow protocol.
OF-CONFIG (OpenFlow Config. and Mgmt. Protocol)	The Configuration and Management Working Group is focused on the core Operation, Administration and Management activities (OA&M) such as bootstrap process, out-of-band network, event reporting, among others. OF-CONFIG allows the configuration and management of OpenFlow datapaths.
Open Transport (Optical Transport Working Group)	Specifies a set of requirements and considerations to control optical and wireless transport networks and devices. It also identifies some use cases in this field.
L4-7 Services	This project describes the architecture of L4-L7 service function chaining (SFC). It also defines the bases or extensions required to SBI and NBI.
Northbound Interfaces (NBI)	Northbound Interface Working Group leverages the development of specific requirements and architectures for NBI.
Wireless & Mobile Working Group	The WMWG aids to identify requirements and use case in wireless and mobile area. This work is focused on the enhancement of Evolved Packet Core (EPC), wireless backhaul, the identification of opportunities in 5G networks, among others.

Table 2: ONF SDN Standardization Activities

SELFNET intends to use the defined standards proposed by ONF, being directly aligned with the ONF reference architecture or the presented Open Datapath, to name a few examples. SELFNET enables a clear separation between the control and data layer, following the reference architecture, and relies in fulfilling its goals by controlling the flow entries in a flow table, like stated in the Open Datapath. SELFNET aims to leverage upon ONF specifications, providing a state of the art implementation of a framework that follows and shares the same goals in the field of SDN. SELFNET will be in a privileged position to not only validate but possibly contribute to ONF standards.

3.1.3. IETF/IRTF

IETF (The Internet Engineering Task Force) and IRTF (Internet Research Task Force) aim to leverage the exploration and standardization of new technologies. There are different efforts and working groups around virtualization and management of current network, as shown in Table 3.

Main Activities	Description
YANG [10]	Yang is a data model language that allows the configuration and control the state data of network Configuration Protocol (NETCONF). Yang models the operations of NETCONF and it could be applied in NFV applications and deployments.
NETCONF [11]	NETCONF protocol defines the rules in order to change and manipulate the configuration of network devices. NETCONF uses well-known technologies such as RPC and XML. NETCONF gains importance in NFV field, where a broader solutions to deploy network function is needed.
SFC (Service Function Chaining) [12]	Provides an architecture for service function chaining. It proposes models, control plane mechanisms, encapsulation schemes, new or extensions protocols involved in the implementation of SFC.
Network Function Virtualization Research Group [13] [14]	NFVRG explores new directions in the development and collaboration of NFV deployments and applications. This group takes into account the benefits of SDN paradigm applied on NFV.
Software Defined Networking Research Group [15] [16]	SDNRG works in the definition of models, interfaces, abstractions, metrics, operation of network devices, protocols, among others, in order to leverage SDN concept.
I2RS Working Group [17] [18]	I2RS defines use cases and a basic architecture based on blocks in order to enhance the routing system (hardware and software) based on a set of interfaces and protocols. I2RS takes into account the SDN and NFV requirements.

Table 3: IETF/IRTF Standardization Activities

Regarding the contribution of SELFNET on IETF/IRTF working groups, SELFNET will take special attention and actively contribute on SDNRG, NFVRG and SFC standardization activities. The definition and adoption of SDN, NFV and SFC on 5G mobile architectures by facilitating the self-management approach is an open challenge. In this context, SELFNET will focus on the upper layers of the different approaches (e.g. SDN Management Plane, SFC Control Plane, NFV Management and Orchestration). In case of I2RS, SELFNET will follow the advances in order to adopt it when necessary. Similarly, the SELFNET development will implement the YANG data model language and NETCONF protocol for the configuration of network devices.

3.1.4. OASIS

Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit organization that promotes the development and adoption of standards related to the information security, Internet of Things, content technologies, emergency management, cloud computing, among others, as shown in Table 4.

Main Activities	Description
TOSCA [19]	Topology and Orchestration Specification for Cloud Applications is a standard language used to orchestrate cloud deployments. Tosca facilitates the coordination of cloud resources (compute and storage). As an example, TOSCA describes whole cycle related to the creation of a new VNF (orchestration process) and the SDN management process.

Table 4: OASIS Standardization Activities

In case of TOSCA work group, SELFNET will contribute in the definition of Network Services (NS) composed by virtual network functions (VNFs) and the corresponding deployment in the virtualized infrastructure. It will enhance the portability of cloud applications and the IT services. This work will be coordinated with other working groups (e.g. ETSI NFV). Similarly, SELFNET will participate on the TOSCA´s revision of the Topology and Orchestration Specification for Cloud Applications.

3.1.5. TM Forum

TeleManagement Forum (TM Forum) is a global association for digital businesses (e.g. service providers, telecom operators, etc.) which provides industry best practices, standards and proof-of-concepts for the operational management systems, also known as Operations Support Systems (OSSs). TM Forum has several working groups running in parallel. Table 5 illustrates the relevant TM Forum working groups from the SELFNET perspective.

Main Activities	Description
ZOOM [20]	The TM Forum Zero-touch Orchestration, Operations and Management (ZOOM) project aims to set the guidelines for service provider support systems which will enable them to provide unprecedented agility, automation and resiliency to the network operations.
FMO [21]	FMO is a TM Forum initiative towards the definition of a new operations architecture, that evolves from the “traditional” BSS/OSS management paradigm to a new approach that leverages on IT

	Operations, DevOps and autonomous control.

Table 5: TM Forum Standardization Activities

SELFNET is, on one side, actively following and aligning its architecture definition with the TM Forum ZOOM and FMO recommendations. Additionally, SELFNET, through one partner of the consortium that is an active member of TM Forum, is also going to actively contribute to the ZOOM working group with respect to the impact that the NFV/SDN paradigm has on the OSSs information model (CFS – Customer Facing Service, RFS – Resource Facing Services, LR – Logical Resources, PR – Physical Resources). Besides the ZOOM working group, SELFNET will also contribute to the FMO working group by participating in the next generation OSS architecture, which includes the autonomic management capabilities to close the autonomic management loop: 1) Supervision – 2) Autonomic – 3) Orchestration/Actuation.

3.2. Relevant Open Source Projects

Due to 5G networks goals and technologies, NFV and SDN became a compelling subject with an emerging community. There are several open source projects to control both NFV and SDN that follow the reference standards provided by ETSI, for NFV and Open Networking Foundation, for SDN. To promote SELFNET's acceptance to the external community, the most community driven implementations are taken into consideration for possible adaptations or integration. So, SELFNET can use these open source projects to avoid repeat problems already addressed, using them as they currently exist or extending them.

3.2.1. NFV Open Source projects

Name	Description
OpenStack [22]	OpenStack is an open source implementation to control and manage virtual infrastructures. It provides multi-tenancy support by isolating the virtual infrastructures of the different tenants. OpenStack control virtualized resources such as virtual disks, machines and networks. OpenStack community is also providing a significant number of components to extend the basic functionality of OpenStack. In particular, OpenStack Neutron provides advanced network capabilities by exposing SDN functionalities to the tenants of the virtual infrastructures. OpenStack Heat provides orchestration capabilities over OpenStack-managed infrastructures. OpenStack Cinder enables advanced storage capabilities by dealing with different highly scalable back-end storage. OpenStack Tacker provides NFV management capabilities over OpenStack. In summary, these OpenStack projects address the management of the ETSI MANO NFV architecture.
OpenMano [23]	OpenMANO is an open source approach to the management and orchestration of ETSI NFV ISG standardization. OpenMANO allows the design of network services and also service instantiation and deletion, it does not provide a VNF Manager. Regarding the VIM it supports multiple VIM instances which can be, not only openvim, but also OpenStack with OpenDayLight as the SDN controller.
Open Source Mano (OSM) [24]	Open Source MANO aims to deliver a production quality MANO stack. OSM provides Service Orchestration, Resource Orchestration and also VNF and NS lifecycle management, it is VIM-independent and is also capable of consuming openly published Information/Data Models. The system offers a Generic VNF Manager (VNFM) and integrates with 3rd party VNFMs so it can be suitable for all VNFs.
OpenBaton [25]	OpenBaton is an ETSI NFV compliant Network Function Virtualization Orchestrator. OpenBaton has a modular implementation with plugins that allow extensibility and the integration without having to modify or understand its core implementation. OpenBaton, natively supports OpenStack as VIM, however, provides a plugin system to incorporate other VIMs. To manage VNFs, OpenBaton provides a generic VNFM and an SDK to develop custom VNFMs.
OPNFV [26]	OPNFV is an open source ecosystem based on standards like ETSI NFV and software to accelerate the development of NFV services. OPNFV targets the NFVI and VIM by connecting projects such as OpenStack or OpenDaylight providing a tested platform to deploy NFV services.

Table 6: NFV Open Source Projects

In SELFNET, all these NFV open source projects are being explored. Currently, OpenStack has been operational in the SELFNET infrastructure platform as the base Virtual Infrastructure Manager. OpenBaton has been employed as the base VNF Manager. Moreover, integration work is underway to operate SFC on the top. Furthermore, SELFNET plans to contribute to these NFV open source projects by providing value-added features achieved in SELFNET, e.g., an integrated Physical and Virtual Infrastructure to accelerate the infrastructure deployment through an automated fashion.

3.2.2. SDN Controllers Open Source projects

Nowadays, SDN and NFV have a robust open source community. With the growing development of these two technologies, including OpenFlow, the number of open source projects are rapidly

increasing, especially regarding SDN controllers. In Table 7 it is shown the different efforts and working groups around SDN controllers Open Source projects.

Name	Description
ODL [27]	OpenDayLight (ODL) project is an industry consortium hosted by The Linux Foundation that it is building an open source framework and platform to accelerate the adoption of SDN and create as well a solid foundation for NFVs. ODL platform makes networks today more configurable and intelligent by improving the programmability of the modern networks and by solving a wide range of common network problems according to the user's needs.
ONOS [28]	ONOS is an Open source SDN networking operating system, addressed to service providers. Intends to provide a platform that eases the development of SDN apps and services. ONOS offers a solid and modular architecture able to scale with high performance and high availability.

Table 7: SDN Open Source Projects

SELFNET is actively following the developments being made on both of them. This awareness will help on the integration of SDN Controllers in the SELFNET architecture. Currently, SELFNET is conducting tests on both SDN Controllers to see which of them is more aligned and suitable with our architecture in order to be integrated on the framework to fulfil our purposes. Thereafter, SELFNET will contribute to the selected open-source SDN Controller by enhancing multi-tenancy capabilities.

3.2.3. Industry Use-Cases Driven Open Source projects

On the industry-side, Central Office Re-architected as a Datacenter (CORD) is one of the most important initiatives.

Name	Description
CORD [29]	CORD stands for Central Office Re-architected as a Datacenter and is a project that aims datacenter cost reduction and cloud agility, targeting network operators, providing reference implementation of a service delivery platform. It's core is built based on ONOS, XOS, OpenStack, and Docker.

Table 8: Industry Use-Case Driven Open Source Projects

SELFNET is following CORD, specifically on the NFV/SDN supervision architecture perspective, also known as A-CORD (Analytics-CORD). SELFNET aims to adopt a similar architecture to A-CORD, based on OpenStack Ceilometer and Monasca (Ceilosca), and enhance it with the integration of legacy network functions and VNFs monitoring and analysis.

3.3. Autonomic Management in NFV/SDN

Novel technologies, such as SDN and NFV are seen as a way to make 5G networks more efficient, more flexible and less costly. In this way, 5G networks will be more programmable. However, one of the main research challenges on adopting SDN and NFV technology is the autonomic management of SDN applications and NFVs.

In an SDN architecture, an SDN controller has the ability to dictate the behaviour of the network devices, by sending rules and control commands to these devices [30]. Autonomic and in-network management approaches offer the capability to migrate management functions to software programs running on the forwarding plane or on the control plane [30].

Currently, there are a lot of efforts being done by mobile operators, standardization organizations and Open Source Projects in order to achieve autonomic management capabilities on the future mobile networks. For example, Snooze [32] is an open-source, scalable, autonomic, and energy-efficient virtual machine (VM) management framework for private clouds. It is similar to other management frameworks such as Nimbus, OpenNebula and OpenStack. Essentially, it allows to build compute infrastructures from virtualized resources. On other hand, there is an ETSI standardization group called AFI GANA [33] [34], which is currently defining a reference model for generic functional blocks, reference points and characteristic information in order to enable autonomics, cognition and self-management in target architectures.

Regarding IETF, there is a research group called "Autonomic Networking Integrated Model and Approach" (ANIMA) [35] which is currently defining an independent and self-managing control plane for autonomic functions.

Regarding 5G networks, one of the main challenges in autonomic management is resource orchestration. It should be implemented a centralized management and orchestration plane that is able to coordinate IT cloud requirements, such as cloud and compute, with networking requirements (e.g. SDN-based WAN) [31]. It is expected that the 5G management and orchestration plane closes the loop between the performance requirements of virtualized service functions and the allocation of

resources exposed by a virtualized distributed heterogeneous substrate [31]. Therefore, automated management is necessary to handle the complexity in the 5G mobile network.

It should also be highlighted that for 5G mobile networks, there are two important concepts to take into account regarding autonomic management: higher availability and higher resilience. The SELFNET approach to deal with these two 5G KPIs is to take advantage of technologies, such as SDN, NFV and artificial intelligence to provide reactive and proactive self-healing capabilities on the 5G mobile network. These self-healing functionalities will detect or predict network failures and malfunctions that are currently being dealt manually or semi automatically by the mobile operators. Therefore, SELFNET will lead to a remarkable reduction upon OPEX and an improvement of QoE/QoS provision in 5G systems in terms of reliability, availability and service continuity [36].

4. SELFNET Reference Architecture & Interfaces

SELFNET will design and implement a Monitoring and Analyzing Subsystem to enable status awareness of the network infrastructure in terms not only of traditional low-level network metrics, but also of a customizable and extensible set of high-level Health of Network (HoN) metrics, which will be taken as a baseline to apply in-depth analysis techniques intended to predict network behaviour. These HoN metrics will enable SELFNET to have more direct and more precise knowledge about the network status, offering a multidimensional view of potential network failures, bottlenecks, security threats, intrusions, etc. SELFNET will enable the automatic deployment of NFV applications in the network infrastructure to facilitate distributed monitoring of the network. These NFV applications are considered as sensors and are intended to obtain low-level metrics from the monitored network elements, and send those metrics to the Monitoring Submodule. Besides the NFV sensors the Monitoring Submodule will also retrieve information from other sources, such as SDN controllers, Virtualization Infrastructure Manager, Data Plane network elements and Physical devices. Once the Monitoring Submodule has gathered the corresponding set of low-level metrics from the different sources, computation of high-level HoN metrics takes place in the Aggregation Submodule. Based on the HoN metrics, the Analyzer Submodule applies several algorithms intended to predict the network behaviour in a use-case driven approach. These predictions are obtained by the use of different techniques and algorithms based on data prediction, data correlation, data mining, machine learning algorithms, etc., applied to the system status in order to produce inferred data from the monitored metrics, such as likelihood to be attacked, system risk values, congestion level, and other predictive metrics that can be used to provide pro-action responses over the network infrastructure. Network behaviour predictions will then be available to the Autonomic Management Subsystem.

4.1. System Architecture

The system architecture defined by SELFNET to address the paradigm described in the previous paragraphs is depicted in Figure 3 [37].

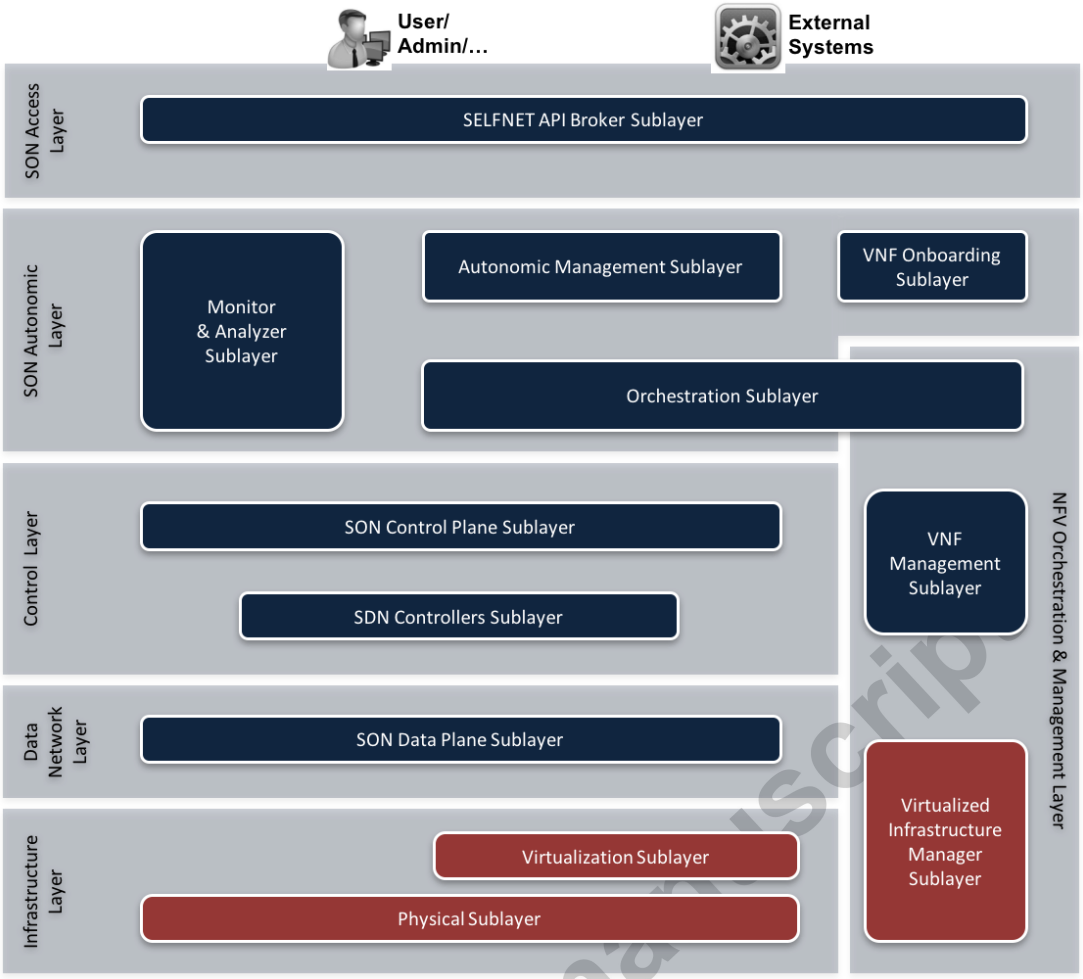


Figure 3: SELFNET System Architecture

Starting from the bottom of the figure, the **Infrastructure Layer (IL)** contains the Physical Sublayer and the Virtualization Sublayer. The **Physical Sublayer** contains all the physical elements of the network, as well as the physical servers available on the Data Center (DC). On top of the Physical Sublayer is provided the **Virtualization Sublayer** which provides access to the virtual resources of the DC (compute, storage and network) through an hypervisor. The Virtualization Sublayer represents the NFVI (Network Functions Virtualization Infrastructure) as defined by the ETSI NFV terminology. It is assumed that a mesh of DCs, with different sizes and purposes, will be available. A number of high-capacity and centralized DCs will exist to host services that do not have significant real-time constraints. In addition to these centralized data centers, edge DCs will also exist in the operator's access networks in order to provide the real-time demanding services and network functions. Distributing network functions across several DCs also requires the system architecture to manage the inter-DCs network links, also known as Wide Area Network (WAN). SELFNET architecture considers support for the described distributed DC topologies by taking into account the inter-DC WAN connectivity, either it is composed by legacy network elements (e.g. MPLS-based routers) or by SDN-enabled/controlled network elements.

On top of the Infrastructure Layer is located the **Data Network Layer (DNL)**, which represents an explicit architectural evolution towards the SDN paradigm. The SDN paradigm decouples the control plane functions from the data plane functions, transforming the latter into a simple forwarding-based layer. Therefore, in order to be fully aligned with SDN, the DNL (more precisely the **SON Data Plane Sublayer**), is explicit in the architecture diagram. This sublayer supports SDN-controlled elements, as well as non-SDN-controlled elements.

To be clear about which type of network functions exist on the DNL, the several types of network functions that are in the scope of SELFNET are presented in Figure 4.

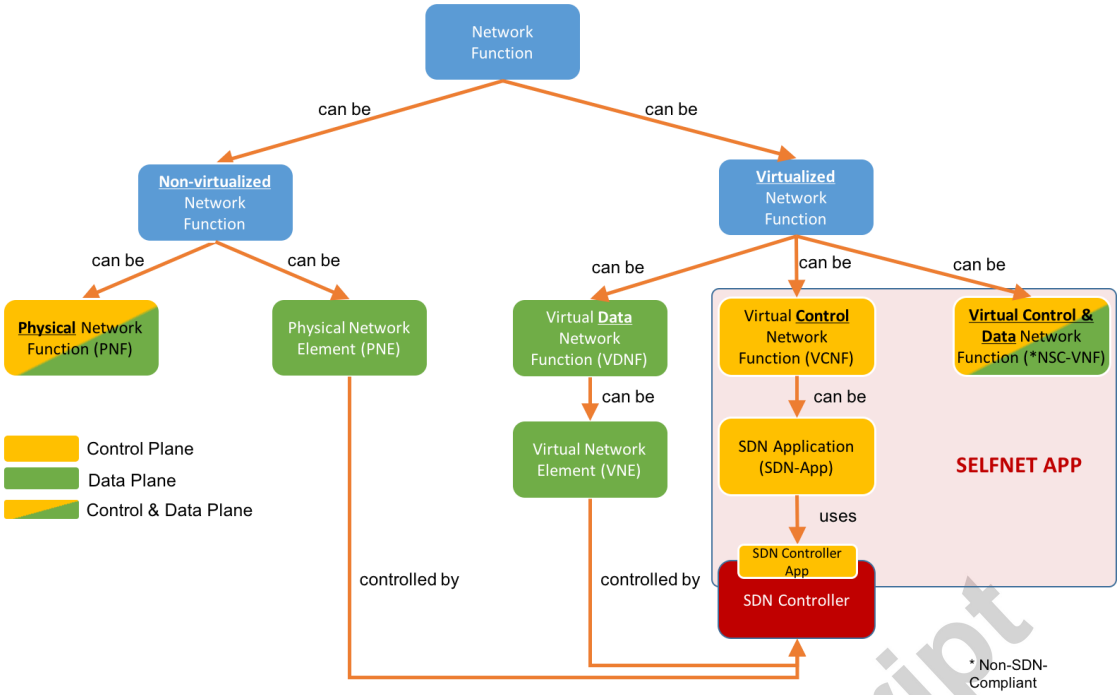


Figure 4: Network Function Types

A network function can be either a non-virtualized network function or a Virtualized Network Function (VNF). When virtualized, the most common model, at least up to now, is to include both control and data plane functionalities, which is not fully compliant with the SDN paradigm since it does not allow the centralized control of its data plane functions. For this kind of virtualized network function, SELFNET refers it to as a Non-SDN-Controllable **Virtual Network Function (NSC-VNF**). A good example is a virtualized Packet Gateway (PGW), which includes control and data plane functions embedded (see Figure 5:). An evolution of this model, which is aligned with the SDN principles, is when the control plane and the data plane functionalities are separated into different logical elements – **Virtual Control Network Function (VCNF)** and **Virtual Data Network Function (VDNF)**, respectively. It's worth mentioning that the relationship between the VNF and the VCNF/VDNF does not have to be 1:1, meaning that a single control plane function (VCNF) can be used to control several data plane network functions (1:N). This is the target model envisaged by SDN in the future. When the VCNF uses the northbound of the SDN Controller, it is usually known as **SDN Application (SDN App)**. In this case, the SDN-App software counterpart required to be deployed on the SDN Controller framework is coined as **SDN Controller App**. When the VDNF is controlled by an SDN Controller, i.e., an SDN-Controllable VNF, the naming proposed within SELFNET is **Virtual Network Element (VNE)**. An example of an SDN App is a Service Chaining Function (SFC), whereas an example of a VNE is a Deep Packet Inspection (DPI) function or a virtual switch, like Open vSwitch (OVS).

On the non-virtualized network functions side, referring to the left side of Figure 4, one can have a **Physical Network Function (PNF)** which comprises data and control plane functionalities or a **Physical Network Element (PNE)** which includes only data plane functionalities. Likewise the VNE, the PNE is aligned with the SDN paradigm and therefore can be controlled by an SDN Controller. An example of a PNF is a 4G eNodeB (eNB), whereas an OVS, when deployed directly on hardware, or a physical switch with OpenFlow support, can be considered as PNEs.

It's also represented in Figure 4 the so-called "SELFNET APP", which is a naming given by SELFNET to all the network functions that can be onboarded to the SELFNET framework. It includes the VCNF, SDN-App, SDN Controller App and the VDNF.

As shown in Figure 5, on the SELFNET DNL is included the PNE and the VNE types, as well as the data component of the PNF and of the VNF, either they represent a sensor or an actuator. On top of the DNL is the **Control Layer (CL)**, which includes two internal sublayers: **SDN Controllers Sublayer** and the **SON Control Plane Sublayer**. The SDN Controllers Sublayer comprises a group of horizontal and vertically distributed SDN Controllers, whereas the SON Control Plane Sublayer represents the network functions control plane, being either actuators or sensors. In terms of the set of network

function types that are embedded in the SON Control Plane Sublayer, the PNF and VNF control components, as well as the SDN-Apps have been identified (see Figure 5).

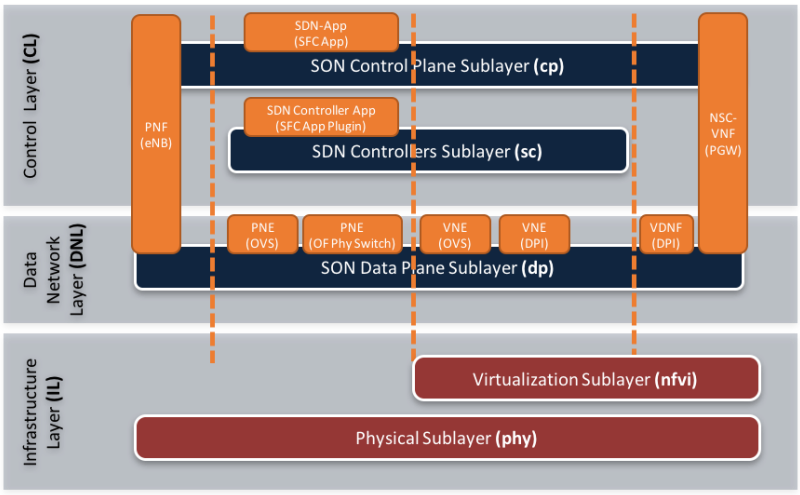


Figure 5: Network Function Types on SELFNET Layered Architecture (with examples)

On the right side of the SELFNET architecture diagram is the **NFV Orchestration and Management Layer (OML)**. It corresponds to the ETSI NFV Management and Orchestration (MANO) layer and is responsible for orchestrating and managing the whole set of virtual functions the are embedded on the SON Control Plane Sublayer and on the SON Data Plane Sublayer. As sublayers, it includes (partially) the **Orchestration Sublayer**, the **VNF Management Sublayer** and the **Virtualized Infrastructure Manager (VIM) Sublayer**. The Orchestration sublayer part in the OML corresponds to the ETSI MANO Network Functions Virtualized Orchestrator (NFVO), and is responsible for orchestrating the virtual resources and network functions. The VNF Management and the VIM sublayers, are responsible for the VNFs and virtual resources management, respectively. These sublayers also correspond to the ETSI MANO VNFM and VIM, respectively.

On top of the already described layers and sublayers are the **SON Autonomic Layer** and the **SON Access Layer**. The SON Autonomic Layer provides the SON intelligent mechanisms, namely:

- Network sensing and SON indicators production – **Monitor & Analyzer Sublayer**;
- Diagnose the network condition and define the set of corrective actions – **Autonomic Management Sublayer**;
- Organized enforcement of the corrective actions on the network (physical/legacy and/or virtual) – **Orchestration Sublayer**;
- Provide new network functions to the SELFNET architecture – **VNF Onboarding Sublayer**;

The topmost layer is the **SON Access Layer**, which encompasses the interface functions that are exposed by the framework. Despite the fact that internal components may have specific interfaces for the particular scope of their functions, these components contribute to a general SON API, managed by the **SELFNET API Broker Sublayer**, that exposes all aspects of the autonomic framework to external actors (Business Support Systems – BSS, Operational Support Systems – OSS and Administration GUI). The GUI provides the network administrator the capability to interact with and configure the framework components (e.g. stop, verify or manually enforce any of the actions that SELFNET is governing) and also obtain the complete status of the network.

4.2. Architecture Interfaces

After describing the SELFNET system architecture in the previous section, the defined interfaces are depicted herein. It's important to mention that although this document defines the system architecture interfaces at the sublayer level, with the progress of the project other interfaces might be required, or the existing ones be modified. Figure 6 illustrates all the SELFNET interfaces that have been identified. Interfaces are organized per sublayer. It is noted that interfaces are bi-directional, although by default the primary exposing/serving end is listed first. Within each sublayer, identified by a specific color, the exposed interfaces and operations to other sublayers are specified. Nevertheless, it should not be excluded the possibility that in certain scenarios the exposing/serving sublayer is also acting as the consumer entity from the counterpart sublayer (and vice-versa).

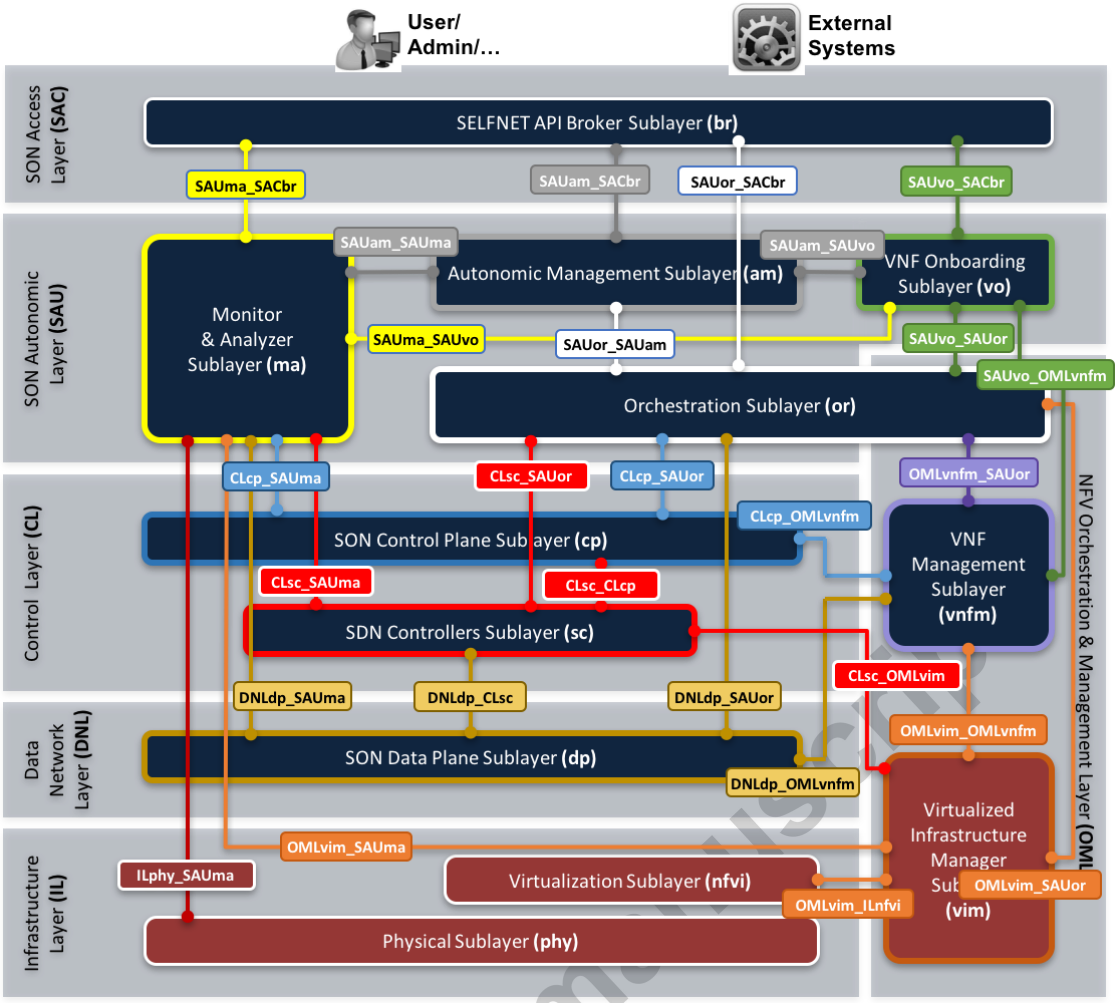


Figure 6: SELFNET Interfaces Overview

For simplicity purposes, the sublayer interfaces are grouped and presented per layer in a table. Table 9 describes the SON Autonomic Layer related interfaces.

Exposing Sublayer	Interface Name	Consuming Sublayer	Interface Summary	SELFNET and/or Standard
VNF Onboarding Sublayer	SAUvo_SACbr	API Broker	APPs lifecycle management (Onboard, modification, offboarding) from the GUI.	SELFNET
	SAUvo_SAUor	Orchestration	Query all data and artefacts for the APPs lifecycle management and configuration.	SELFNET
	SAUvo_OMLvnfm	VNFM	Query all data and artefacts for the APPs lifecycle management and configurations.	SELFNET
Orchestration Sublayer	SAUor_SACbr	API Broker	Self-* action enforcements on the network from the GUI.	SELFNET
	SAUor_SAUam	Autonomic Management	Self-* action enforcements on the network from the autonomic component.	SELFNET
Monitor & Analyzer Sublayer	SAUma_SACbr	API Broker	Monitoring information to the GUI (per tenant).	SELFNET
	SAUma_SAUvo	VNF Onboarding	Provisioning of new onboarded APPs to be monitored.	SELFNET
Autonomic Management Sublayer	SAUam_SAUma	Monitor & Analyzer	Health of network SON indicators provided to the decision making algorithms.	SELFNET
	SAUam_SACbr	API Broker	SELFNET actions lifecycle management.	SELFNET
	SAUam_SAUvo	VNF Onboarding	Provisioning of new onboarded APPs/actions.	SELFNET

Table 9: SELFNET SON Autonomic Layer Interfaces Summary

Table 10 describes the NFV Orchestration & Management Layer related interfaces.

Exposing Sublayer	Interface Name	Consuming Sublayer	Interface Summary	SELFNET and/or Standard
VNFM Sublayer	**OMLvnfm_SAUor**	Orchestration	VNF lifecycle management (deploy, start, stop, etc.).	ETSI NFV MANO Or – vnfm & SELFNET-enhanced
VIM Sublayer	**OMLvim_SAUor**	Orchestration	Virtualized compute and network resources management, as well as service chaining management.	ETSI NFV MANO Or – vi & SELFNET-enhanced
	OMLvim_vnfm	VNFM	Virtualized compute and network resources management.	ETSI NFV MANO Vi – vnfm & SELFNET-enhanced
	OMLvim_SAUma	Monitor & Analyzer	Virtualized compute and network resources monitoring.	ETSI NFV MANO Or – vi & SELFNET-enhanced
	OMLvim_ILnfvi	NFVI	Virtualized compute and network resources management.	ETSI NFV MANO Nf-Vi & SELFNET-enhanced

Table 10: SELFNET NFV Orchestration & Management Layer Interfaces Summary

Table 11 describes the SON Control Layer related interfaces.

Exposing Sublayer	Interface Name	Consuming Sublayer	Interface Summary	SELFNET and/or Standard
Control Plane Sublayer	**CLcp_SAUor**	Orchestration	Control plane functions configuration.	SELFNET
	CLcp_SAUma	Monitor & Analyzer	Control plane functions monitoring.	SELFNET
	CLcp_OMLvnfm	VNFM	Control plane functions basic configuration and operational management.	ETSI NFV MANO Ve-Vnfm-em and Ve-Vnfm-vnf & SELFNET-enhanced
SDN Controllers Sublayer	**CLsc_SAUor**	Orchestration	Orchestrator pushes flow control etc. requirements to SDN controller; Orchestrate manages the lifecycle of SDN Controller Apps	SDN Controller Northbound specific & SELFNET-enhanced
	CLsc_CLcp	Control Plane Functions	SDN-Apps push application (flow control etc.) requirements to SDN controller	SDN Controller Northbound specific & SELFNET-enhanced
	CLsc_SAUma	Monitor & Analyzer	Monitor & Analyzer collects SDN controller's status/metrics	SDN Controller Northbound specific & SELFNET-enhanced
	CLsc_OMLvim	VIM	Similar to that of **CLsc_SAUor**	SDN Controller Northbound specific & SELFNET-enhanced

Table 11: SELFNET Control Layer Interfaces Summary

Table 12 describes the Data Network Layer related interfaces.

Exposing Sublayer	Interface Name	Consuming Sublayer	Interface Summary	SELFNET and/or Standard
Data Network Sublayer	**DNLdp_SAUma**	Monitor & Analyzer	Data plane functions monitoring	SELFNET
	DNLdp_CLsc	SDN Controller	SDN controller enforces rules in the data plane	OpenFlow, NetFlow
	DNLdp_SAUor	Orchestration	Data plane functions configuration.	SELFNET
	DNLdp_OMLvnfm	VNFM	Data plane functions basic configuration and operational management.	ETSI NFV MANO Ve-Vnfm-em and Ve-Vnfm-vnf & SELFNET-enhanced

Table 12: SELFNET Data Network Layer Interfaces Summary

5. SELFNET Use-Cases Workflows

This section highlights the workflow across the various interfaces for operations that are related to the SELFNET use-cases.

5.1. Proactive self-healing for resource/power supply and App aging

The Self-Healing (SH) in SELFNET goes beyond the traditional definition that follows a "Break and Fix" approach. SH use case focuses not only on reactive measures to deal with faulty network elements and infrastructure resources (e.g., physical/virtual servers), but also on proactive actions that improve resilience, availability and safety on the network infrastructure.

This primary SH scenario addresses the need of constant monitoring of the network infrastructure. For instance, it is important to monitor the power output and the temperature of the network equipment in order to trigger alarms allowing proactive healing actions to be applied to correct malfunctions before they lead to a serious outage. One of the biggest innovations in this SH scenario is the use of context-aware information in the Control Plane and the detection of vulnerabilities on the virtual execution environment that will enhance the SH capabilities of SELFNET.

To accomplish the primary scenario of the self-healing use case, firstly SELFNET will deploy self-healing SDN/NFV sensors to collect metrics (e.g., virtual resource utilization) from the management plane of the infrastructure. Moreover, environmental data will be collected periodically, by the SON sensors at the Control Layer, and aggregated at the Monitor & Analyzer sublayer, which will have to be able to correlate, enrich and provide real-time analysis. In this way, The Monitor & Analyzer sublayer will collect and store all data in order to infer Health of Network (HoN) state and infrastructure metric reports and send them to the Autonomic manager module. Then, the Autonomic Management sublayer, which is the intelligent module of the SELFNET framework, will use artificial intelligence, data mining and stochastic algorithms to diagnose network problems (in this scenario, e.g., energy overuse or failing, server overheating, App aging etc.) and decide the best strategy to be taken so that the problems could be mitigated. These decisions (typically in terms of selected Apps and configurations) are passed to the Orchestration sublayer, which is in charge of the real deployment of SH NFV/SDN apps, where the availability of resources (virtual and/or physical) required by the detailed plan is checked. If sufficient resources are available, SELFNET will deploy actuators to strengthen the robustness of the network infrastructure and sustain its performance. In this SH scenario, the actuators are deployed in the form of App Rejuvenators, Energy Managers and Power Controller's Apps. In Figure 7, it is demonstrated the workflow of the SH Use case scenario described above.

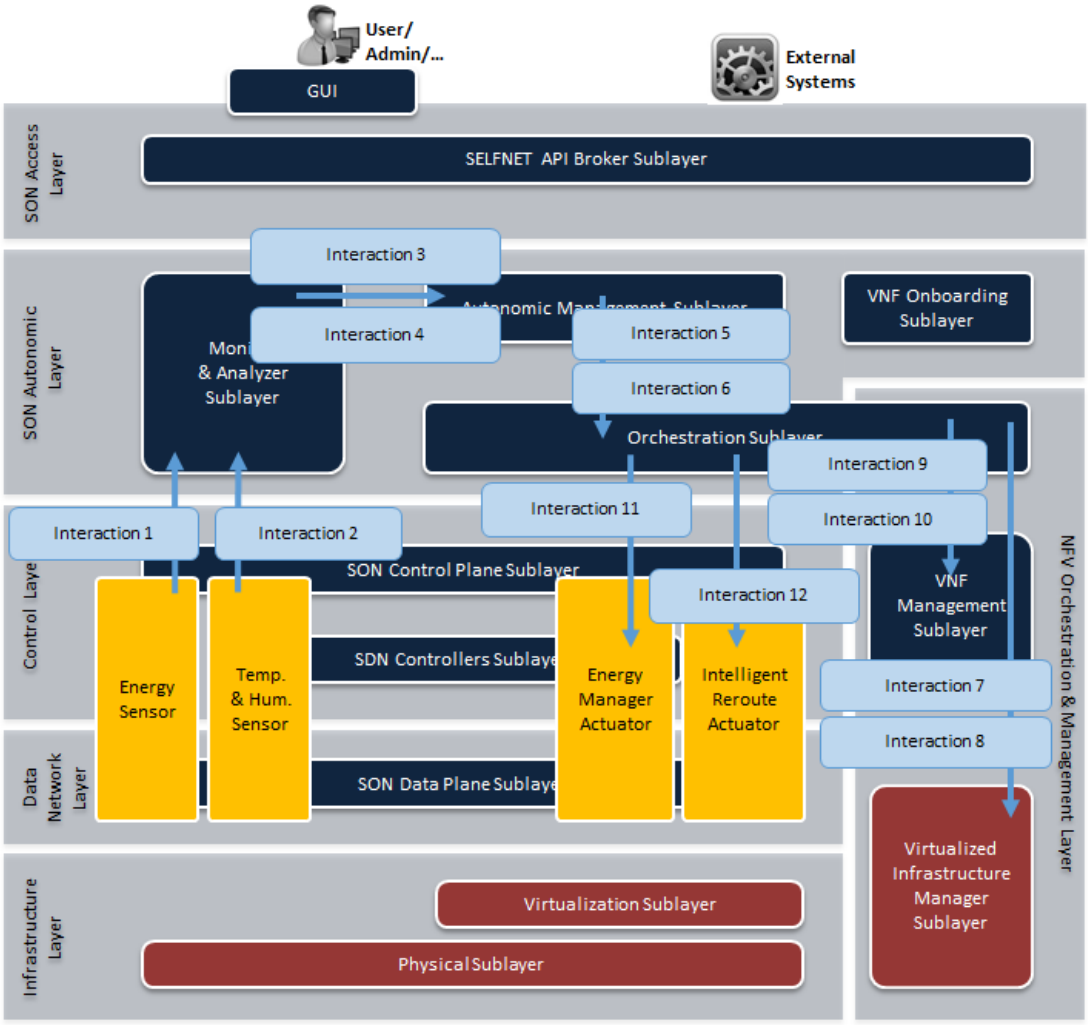


Figure 7: Self-Healing Use Case Workflow

Table 13 provides detailed information about the SH use-case interactions.

Self-Healing Workflow			
Step	**Operation Name**	**Triggering Reason & Input Information**	**Expected Result & Output Information**
1 & 2	Sensor Information Report	Threshold defined exceeded (e.g.: low 70%, medium 80% and high 90%) Input: Output power (energy) values, Temperature and Humidity values;	Trigger an alarm/event/risk in Monitor & Analyzer sublayer Output: Alarm level and Energy/Temperature/Humidity values from location X;
3 & 4	Situation Awareness Report	Medium/High Energy consumption detected on server equipment Y; Medium/High Temperature detected on network equipment Y; Input: Energy values, Temperature and Humidity values;	Solve Energy consumption problem on server equipment Y; Solve Temperature/Humidity problem on network equipment Y; Output: Location X, equipment Y, tenant ID, alarm type;
5 & 6	Action Plan Report	Detected Energy consumption problem on server equipment Y; Deploy action plan I: Migrate everything from Y to Z then shutdown Y for later maintenance; Input: Location X, equipment Y, tenant ID, action plan I; Detected temperature problem on equipment	Identify the best action(s) from the plan I/P; Adequate resource allocation for the selected action(s); Chosen Action(s) from plan I/P: (ex: deploy VNF Energy Manager/ deploy VNF Intelligent Reroute), location X, equipment Y,

		Y Deploy action plan P: Deploy SDN app and redirect traffic to another equipment Z and then shutdown Y for later maintenance; Input: Location X, equipment Y, tenant ID, action plan P;	routing parameters, equipment Z tenant ID;
7 & 8	Reserve Virtual Resources	VNF Energy Manager/VNF Intelligent Reroute deployment action(s) is required Input: Tenant Identifier, Resource Description, Location Identifier, Security Group Identifier	Reserve the required virtual resources to deploy the action plans requested by the Autonomic Management sublayer Output: Virtual resources to be used for VNF instantiation
9 & 10	VNF Instantiation	Instantiate VNF Energy Manager/VNF Intelligent Reroute Input: VNF descriptor, tenant ID	VNFs running Output: VNF Identifier
11 & 12	Configure Control APP	Apply action(s): deploy VNF Energy Manager; deploy VNF Intelligent Reroute; Input: Location X, equipment Y, equipment Z, tenant ID;	Configure new resources for the allocation of the chosen action(s) Output: APP status

Table 13: Self-Healing Workflow Interactions

5.2. DDoS attacks conducted by a botnet

SELFNET enables the detection and mitigation of network traffic congestion caused by potential cyber-attacks. The expected large number of subscribers in 5G networks provides a new opportunity to compromise a huge amount of devices, which in turn allows attackers to trigger much larger attacks. The aim is therefore to increase security, resilience, and service continuity of advanced scalable self-protection network security mechanisms and techniques.

The primary SELFNET self-protection scenario aims to safeguard 5G networks from Distributed Denial of Service (DDoS) conducted by a botnet. Due to the large number of high bandwidth connected devices envisaged with 5G, monitoring of raw network packets to enable Deep Packet Inspection (DPI) is practically unfeasible. An approach based on two levels of abstraction is therefore needed to detect botnets. First, a high level and fast detection is performed by only monitoring network traffic flows from the 5G edge and core networks. Once potential attacks are being detected (e.g. command and control channels), a number of DPI specialized tools are strategically deployed to confirm the suspect of attacks. This enables a second step of low level detection at the packet level, and when a botnet is actually detected and confirmed, a final reaction is triggered to mitigate the attack, e.g. by means of virtualized and personalized honeynets to be deployed at the proper network location to protect users against the cyber-attack, and learn from it while diverting affected traffic to separated controlled networks (i.e. honeynets) where the attack can be isolated.

A pool of high level sensors is initially deployed to gather raw network packages in order to monitor the existence of command and control (C&C) communication channels. These high level sensors will not apply inspections at packet level, and will only provide to the Monitor & Analyzer module monitoring information at the granularity of the network traffic flows. When potential command and control channels are detected, a correspondent HoN metric is forwarded to the Autonomic Manager to compute the reaction plan and request the allocation and deployment of new low level inspection sensors. The Orchestrator picks the proper IDS sensor (i.e. a virtual DPI tool in the form of SDN or VNF application) and takes care to instantiate and configure them to enable the second round of attack detection at a finer granularity. This second round of detection follows the same approach of the high level one, and alerts and low level detection information are sent to the Monitor & Analyzer to let it identify and confirm the detection of a botnet. When a botnet is finally detected, the Autonomic Manager sends a second detailed plan to the Orchestrator to deploy a personalized virtual honeynet, which replicates the affected hosts and network with the aim of isolating the attack. Here an additional application to reconfigure the network flow tables to divert affected traffic to the virtual honeynet has also to be deployed.

Figure 8 shows the self-protection workflow described above detailing interactions among components of the SELFNET architecture.

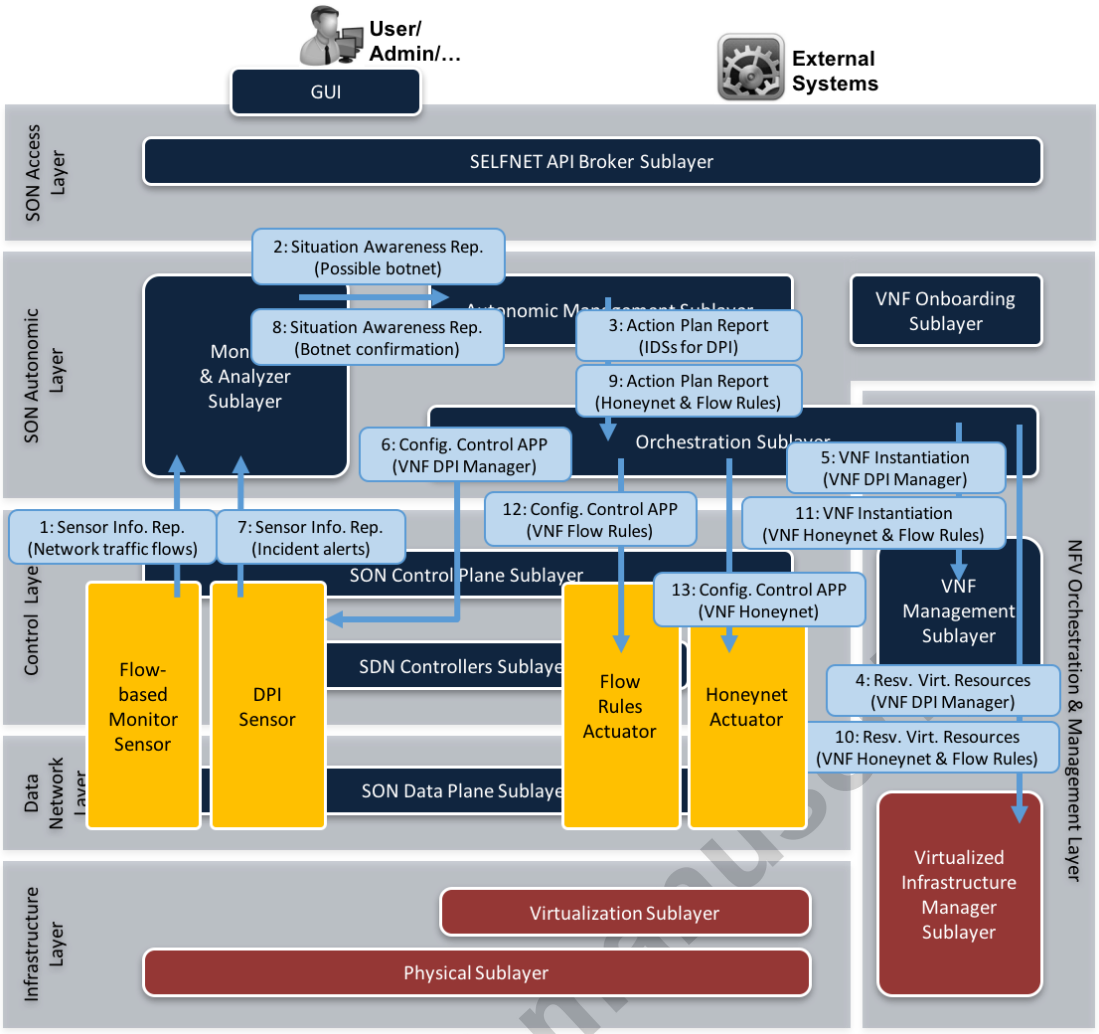


Figure 8: Self-Protection Use Case Workflow

A step-wise description of each interaction is provided in Table 14.

Self-Healing Workflow			
Step	**Operation Name**	**Triggering Reason & Input Information**	**Expected Result & Output Information**
1	Sensor Information Report	Flow-based monitoring sensor is continuously monitoring 5G edge and core network elements Input: Raw network packages	Status of network traffic flows Output: Congestion situation and number of packets from/to a given host
2	Situation Awareness Report	High network congestion or suspected communication links between a given number of hosts Input: Network traffic flows from high-level detection sensors	Potential C&C channel detected Output: Affected devices' information (e.g., IP addresses)
3	Action Plan Report	Detected an alleged C&C channel shaping a botnet Input: Devices' information (e.g., IP addresses) shaping the botnet	Selection of appropriate low-level sensor apps (virtual IDSs) from repository to be deployed Output: List of actions to deploy a number of low level sensors with their specific configuration
4	Reserve Virtual Resources	DPI VNF deployment action is required Input: virtual IDSs' allocation request, Tenant ID, Resource Description	Virtual resources for deploying and enforcing the virtual IDSs for DPI reserved Output: virtual resources identifiers for VNF instantiation
5	VNF instantiation	Request to instantiate a DPI VNF Input: VNF descriptor, Tenant ID	DPI VNF is instantiated and properly running Output: VNF Identifier

6	Configure Control APP	DPI VNF configuration request to apply virtual IDSs rules Input: virtual IDSs specific configuration, Tenant ID	virtual IDSs configured to support DPI and ensure the existence of a botnet suspect Output: Status message
7	Sensor Information Report	Low-level virtual IDSs configured upon possible C&C channel detected during the implementation of step 1 Input: Raw network packages from virtual IDSs	Confirmation of the botnet detection Output: Alerts reporting incidents on a cyber-attack
8	Situation Awareness Report	A botnet (e.g., its C&C communication channels) has allegedly been detected Input: Alerts reporting the existence of a list of C&C communication channels, which form a botnet	Request for a reaction to the detected botnet with the aim of diverting affected traffic Output: List of threat sources (compromised devices, i.e. bots), their victim(s) and the C&C server's location
9	Action Plan Report	Detection of the botnet that was allegedly identified during step 3 Input: List of threat sources (bots), their victim(s) and the C&C server's location	Selection of appropriate virtual honeynet-related apps from repository Output: List of actions to deploy a virtual honeynet and enforce new flow tables to divert affected traffic
10	Reserve Virtual Resources	Honeynet and Flow Rules VNF deployment action is required Input: new flow table rules to divert the C&C communications, Tenant ID, VNFs Description	Virtual resources for deploying and enforcing the virtual honeynet reserved Output: virtual resources identifiers for honeynet and Flow Rules VNFs instantiation
11	VNF instantiation	Request to instantiate Honeynet & Flow Rules VNFs Input: VNF descriptor, Tenant ID	Honeynet & Flow Rules VNFs running Output: Honeynet and Flow Rules VNFs Identifier
12 & 13	Configure Control APP	Request to configure honeynet and Flow Rules VNFs Input: Threat sources (bots), victim(s), routing parameters, VNFs configuration, Tenant ID	Flow table rules reconfigured to redirect affected traffic to the honeynet configured to clone the threat sources and their victim(s) Output: Status message

Table 14: Self-Protection Workflow Interactions

5.3. Video Streaming in Changing Network Environment using a 5G Hot Spot

The SELFNET Self-Optimization use case focusses on improving the 5G user experience by addressing the requirement to maintain acceptable levels of video quality through the use of video adaptation techniques and development of new QoE metrics at both video stream and network levels. It will also contribute to help achieving the low latency 5G KPI at the application level by meeting the real time requirements of video services. 5G Business Model requirements will be addressed by demonstrating underpinning technologies for potential new high value, high quality video services including support for new U-HD (Ultra-High Definition) video applications.

This particular scenario a nomadic mobile user enters a busy public location such as a cafe, arena or airport where he connects to a 5G hot spot. There are a number of other users connected to the same 5G hot spot, all of whom use Internet access for a diverse set of tasks including social media networking, video watching, e-mail and VPN access using their smartphones, tablets and laptops. It is assumed that there will be a number of adjacent hot spots, some of which offer overlapping coverage. He has requested a U-HD video stream from a content provider located out with his own network.

This use case is exercised across the SELFNET framework by deployment of sensors able to acquire data on the video streams passing through the network and on the current state of the network. A set of video sensors detect the presence of a new video flow and acquire detailed information on the video stream either from out of band metadata such as a video descriptor file or directly from the video stream itself (Step 2 in Table 15 and Figure 9). The network state sensor, a common requirement across all use cases, continuously monitors current network conditions (Step 1 in Table 15 and Figure 9). Further sensors monitor the energy usage (Step 3 in Table 15 and Figure 9) of components (in this example the 5G hotspot access points) and provide collect information on user device capabilities and user preferences (Step 4 in Table 15 and Figure 9)regarding the priority of application they are currently running.

The Sensor Information reports (Steps 1 to 4 in Table 15 and Figure 9) are passed to the SELFNET monitor/analyser where the impact on user QoE of the video stream characteristics and the current network state is analysed. The result of this analysis is given in situation awareness reports detailed (Steps 5 & 6 in Table 15 and Figure 9) for the actual or predicted QoE of video flows at a particular

location (in this case the public location where the 5G hotspot is located) and energy usage. Where these reports indicate a predicted drop in QoE (expressed by means of a new video HoN metric), the Autonomic Management sublayer determines the cause of any current, or predicted, drop in estimated QoE and establishes and a detailed plan (Steps 7 & 8 in Table 15 and Figure 9) prepared to allocate resources required to mitigate the measured/anticipated reduction in QoE. The plan is passed to the orchestrator where the availability of both physical and virtual resources required by the detailed plan is checked. Where sufficient resources are available the actuators described in the plan are deployed and configured (Steps 9 to 14 in Table 15 and Figure 9) in the form of, for example Media Aware Adaptation Entity (MANE) NFV Apps.

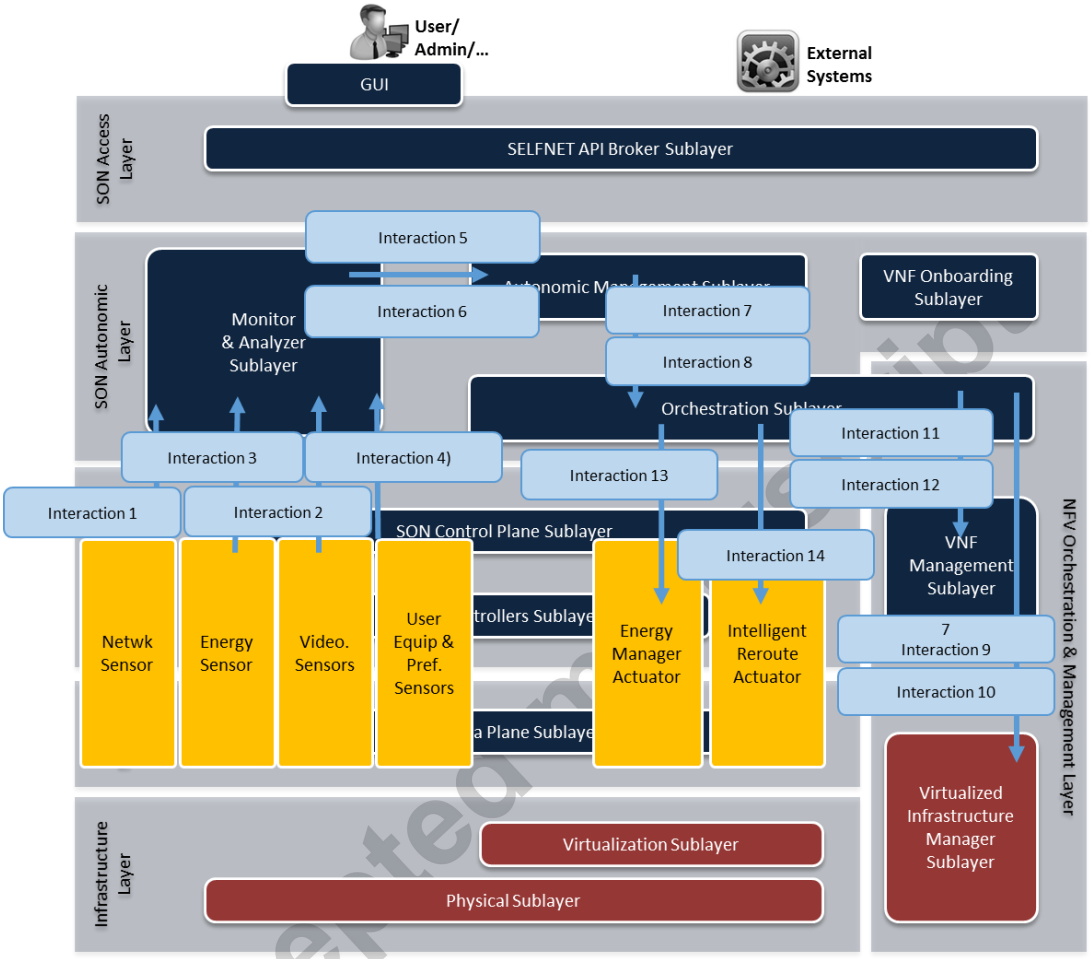


Figure 9: Self-Optimization Use-Case Workflow

A step-wise description of each interaction is provided in Table 15.

Self Optimisation Workflow			
Step	**Operation Name**	**Triggering Reason & Input Information**	**Expected Result & Output Information**
1..4	Sensor Information Report	New video flow detected Input: Network metrics (1), Video flow descriptors (2), energy usage (3) & user preferences/device capabilities(4)	Trigger an alarm/event/risk in Monitor & Analyzer sublayer Output: Network metrics, video stream descriptors, energy usage & UE preferences for video flow A at location X
5,6	Situation Awareness Report	Video Quality HoN metric has fallen (or predicted to fall) below threshold Input: Video HoN value;	Resolve video quality degradation problem for video flow A at location X; Output: Video Flow A, Location X, alert type;
7,8	Action Plan Report	Detected reduction in actual/predicted video quality in video flow A at location X; Deploy action plan I: Apply corrective measures to restore video quality of flow A	Identify the best action(s) from the plan I; Adequate resource allocation for the selected action(s); Chosen Action(s) from plan I:

		at location X Input: Location X, video flow A, action plan I;	(ex: deploy VNF MANE (7)), location X, video flow A; Or switch on/off AP K in location X and transfer flow A to AP K (8)
9,10	Reserve Virtual Resources	VNF MANE/VNF AP actuator deployment action(s) is required Input: Video Flow Identifier, Resource Description, Location Identifier, Resource (AP) Identifier	Reserve the required virtual resources to deploy the action plans requested by the Autonomic Management sublayer Output: Virtual resources to be used for VNF instantiation
11,12	VNF Instantiation	Instantiate VNFMANE/VNF AP actuator Input: VNF descriptor, tenant ID	VNFs running Output: VNF Identifier
13,14	Configure Control APP	Apply action(s): deploy VNF MANE / VNF AP actuator; Input: Location X, Video Flow A;	Configure new resources for the allocation of the chosen action(s) Output: APP status

Table 15: Self-Optimization Workflow Interactions

6. Integration of Standards and Open Source Projects in SELFNET Architecture

Figure 10 presents the interactions between the SELFNET framework described in Section 4 and the most relevant STOs and open source projects (in italic). It maps the SELFNET architecture with the standards and open source projects being explored in SELFNET. On one hand, it shows the influence (incoming arrows) of these standards and projects on the definition and development of the corresponding components in the SELFNET framework. On the other hand, it indicates the potential contributions (outgoing arrows) from SELFNET to the standardization activities and open source projects development. In the subsequent subsections, we describe both perspectives following a bottom-up approach aligned with the SELFNET architecture.

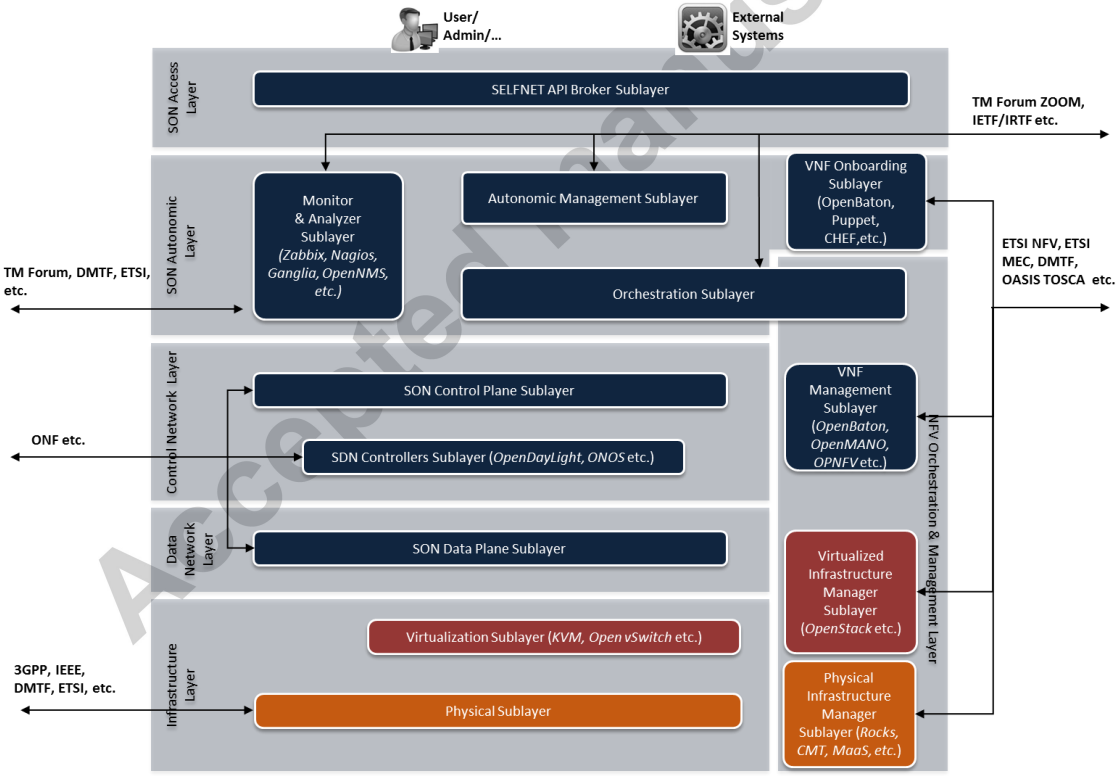


Figure 10: Alignment of SELFNET and related STOs and open projects

6.1 Infrastructure Deployment and Management

For the Physical sublayer, SELFNET is mainly underpinned by the ongoing standardization from mobile/cellular telecommunication STOs such as 3GPP/ETSI. When offloading from 5G to WiFi is considered for SELFNET use cases such as Self-optimization and Self-healing, IEEE standards also come into play. Since the focus of SELFNET is the management plane of 5G networks, innovation at the physical level (air interface, spectrum allocation etc.) for 5G networks is largely beyond the scope.

Meanwhile, SELFNET envisions and endeavors to prototype the next-generation infrastructure to be based on a Mobile Edge Computing (MEC) paradigm, where cloud-based, virtualized networking and computing resources and capabilities are distributed at the edges of 5G networks, in line with the vision by the ESTI MEC ISG [38] and the ESTI NFV ISG [39]. Therefore, SELFNET intends to make a significant contribution to the standardization activities related to MEC and NFV through ETSI or other related STOs such as DMTF. Specifically, it is foreseen that a major innovation would originate from an automated, prompt and dynamic deployment of the MEC infrastructure, currently under development in SELFNET. This automated MEC deployment is enabled by integrating system-level automation in installing operating systems, software packages, services etc. from scratch on top of bare metal hardware, coupled with physical and virtualized infrastructure management capabilities offered by related open source projects such as Cluster Rocks [40], HP Insight Cluster Management Utility [41], MaaS [42], OpenStack [22]. Consequently, speedy infrastructure deployment will be realized, which will contribute to achieving one of the 5G KPIs in terms of substantially reducing the service creation time (from 90 days to 90 hours). In addition, such a capability would also help the Self-healing of the infrastructure in major disruptive scenarios.

6.2 SDN Networking and Control

As shown in Figure 5.1, the combined Data and Control Network layers are fully compliant with the three-layer SDN architecture [43] defined by ONF. For the SON Data Plane sublayer, corresponding to the ONF SDN Infrastructure layer, open source based SDN devices such as Open vSwitch [44] will be employed in SELFNET. For the SDN Controllers sublayer, equivalent to the ONF SDN Control layer, SELFNET is exploring SDN controllers based on open source project such as OpenDayLight [27] or ONOS [28]. Finally, for the SON Control Plane sublayer, or the ONF SDN Application layer, SDN sensor/actuator Apps will be developed, some of which can be built upon existing open source tools (e.g., from [45]) wherever appropriate.

Clearly, ONF is the primary STO to be targeted for standardization contributions in the SELFNET SDN domain. For the Southbound API of the SDN controller, standard communication protocols such as OpenFlow and the standard SNMP will be reused and maybe improved for the interactions with the SDN devices. For the Northbound, the ONF RESTful Northbound Interface for real-time media [39] is being considered for the SELFNET Self-Optimization use case in handling video applications, and extensions may be made in the context of 5G networking conditions. Other potential contributions to standards may include enhanced multi-tenancy support for SDN Apps, optimization techniques for SDN service function chaining and so on.

6.3 VNF Onboarding, and NFV Orchestration and Management

The encapsulation, onboarding and management of VNF in SELFNET has been strongly influenced by the relevant open source projects especially OpenBaton [25], OpenMANO [23] and OPNFV [26]. These projects provide starting points of developments in order to enable SELFNET to cope with the management of VNF while achieving the ambitious 5G KPIs. Management and orchestration of NFVs are now being actively considered in both ETSI NFV and MEC ISG. SELFNET is clearly planning to contribute to such STOs. Regarding onboarding and encapsulation mechanisms, although there are some existing approaches such as those provided by traditional Configuration Management Tools e.g., Puppet [47], CHEF [48], Ansible [49] or Juju [50] and the approach provided by OpenBaton [25], SELFNET plans to provide a significant step forward in this direction considering specific requirements related to Mobile Edge Infrastructures such as multi-tenancy and multi-location capabilities. These innovations could also be submitted to DMTF and OASIS TOSCA STOs.

6.4 SON Autonomic Layer

From the network management perspective, SELFNET is largely influenced by STOs such as DMTF and TM Forum regarding standards for network management and operational service support. SELFNET is considering as the starting point of a number of different open source projects for monitoring, network inventory management and operational information management such as OpenNMS [51], Nagios [52], Ganglia [53] and Zabbix [54], among others.

SELFNET intends to provide significant contributions to enhancing the current network intelligence of 5G networks. Consequently, SELFNET considers liaising with TM Forum Zoom and IETF/IRTF in order to contribute in the area of network intelligence and autonomic management in these STOs.

7. Conclusions and Future Work

SELFNET is a scalable, extensible and smart network management architecture which explores the integration of technologies, widely recognized as key enabling technologies for 5G systems, such as SDN, NFV, Self-Organizing Networks (SON), Cloud Computing, and Artificial Intelligence to implement an autonomic network management system addressing a number of management tasks, such as network monitoring, maintenance, service provisioning and deployment of tools. The paper presented an overview of the architecture which aims to meet the requirements of future network management tasks. The implementation of the framework is based on available and evolving industry standards and re-uses well supported open source products. The current and future work focuses on the implementation and demonstration of the framework capabilities of self-optimization, self-healing and self-protection, and its validation based on use cases. Two testbeds will be deployed, one in Scotland and another one in Portugal, to deploy and validate the results of the proposed SELFNET architecture. The experience so far suggests that valuable contributions can be brought into the evolving standardization work in groups such as ETSI NFV. Further future work includes the validation of the framework in large scale environments, in the scope of vertical industry cases and operators' environments, in order to draw conclusions on the scalability of the framework and its suitability in a business environment. The ambition is to provide the framework as a basis for large-scale trials in the scope of the second phase of the 5G-PPP.

Acknowledgments

This work was funded by the European Commission Horizon 2020 5G-PPP Programme under grant agreement number H2020-ICT-2014-2/671672 – SELFNET (Self-Organized Network Management in Virtualized and Software Defined Networks). The authors wish to thank all the SELFNET partners for their support in this work.

References

[1] EU SELFNET Project – Self-Organized Network Management in Virtualized and Software Defined Networks. Project reference: H2020-ICT-2014-2/671672. Funded under: H2020. Available at http://www.selfnet-5g.eu

[2] SELFNET Deliverable 2.1 - Use Cases Definition and Requirements of the System and its Components. Main Editors: Luis Javier García Villalba, Ángel Leonardo Valdivieso Caraguay, Lorena Isabel Barona López, from Universidad Complutense de Madrid. Available at https://selfnet-5g.eu/dissemination/

[3] Pedro Neves et. Al, "The SELFNET Approach for Autonomic Management in an NFV/SDN Networking Paradigm", International Journal of Distributed Sensor Networks, Volume 2016 (2016).

[4] ETSI GS NFV 002 V1.2.1, "Network Functions Virtualisation (NFV); Architectural Framework", ETSI NFV ISG, December 2014

[5] ETSI GS NFV-MAN 001 V1.1.1, "Network Functions Virtualisation (NFV); Management and Orchestration", ETSI NFV ISG, December 2014.

[6] ETSI GS NFV-SWA 001 V1.1.1, "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture", ETSI NFV ISG, December 2014

[7] ETSI GS NFV-EVE 005 V1.1.1, "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework", ETSI NFV ISG, December 2015

[8] "Open Networking Foundation," 2016. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/about/onf-what-why-2016.pdf

[9] "Open Networking Foundation: Technical Library". [Online]. Available: https://www.opennetworking.org/sdn-resources/technical-library

[10] "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)". IETF RFC 6020. [Online]. Available: https://tools.ietf.org/html/rfc6020

[11] "Network Configuration Protocol (NETCONF)". IETF RFC 4741 [Online]. Available: http://www.rfc-base.org/txt/rfc-4741.txt

[12] "Service Function Chaining". [Online]. Available: https://datatracker.ietf.org/wg/sfc/charter/

[13] D. Lopez and R. Krishnan: "The NFVRG Network Function Virtualization" [Online]. Available: http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_313.pdf

[14] "Network Function Virtualization Research Group". [Online]. Available: https://irtf.org/nfvrg

[15] “Software-Defined Networking (SDN): Layers and Architecture Terminology” [Online]. RFC 7426. IETF Available: https://tools.ietf.org/html/rfc7426
[16] “Software-Defined Networking Research Group SDNRG”. [Online]. Available: https://irtf.org/sdnrg
[17] “An Architecture for the Interface to the Routing System”, IRTF, draft version 13. [Online]. Available: https://tools.ietf.org/html/draft-ietf-i2rs-architecture-13
[18] “Interface to the Routing System”. [Online]. Available: https://datatracker.ietf.org/group/i2rs/charter/
[19] “OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC”. OASIS. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
[20] TM Forum Zoom, [online], available at https://www.tmforum.org/zoom/
[21] TM Forum FMO, [online], available at http://inform.tmforum.org/tag/fmo/
[22] OpenStack, [online], available at https://www.openstack.org/
[23] OpenMANO, [online], available at https://github.com/nfvlabs/openmano
[24] OpenSourceMano, [online], available at https://osm.etsi.org
[25] OpenBaton, [online], availale at http://openbaton.github.io/
[26] OPNFV, [online], available at https://www.opnfv.org/
[27] OpenDayLight, [online], available at https://www.opendaylight.org/
[28] ONOS, [online], available at http://onosproject.org/
[29] CORD, [online], available at https://wiki.onosproject.org/pages/viewpage.action?pageId=3441030
[30] Wickboldt, Juliano Araujo, et al. "Software-defined networking: management requirements and challenges." IEEE Communications Magazine 53.1 (2015): 278-285.
[31] 5G PPP Architecture Working Group, View on 5G Architecture, [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-For-public-consultation.pdf
[32] Feller, Eugen, Louis Rilling, and Christine Morin. "Snooze: A scalable and autonomic virtual machine management framework for private clouds."Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012). IEEE Computer Society, 2012.
[33] Chaparadza, R., et al. "Implementation Guide for the ETSI AFI GANA Model: a Standardized Reference Model for Autonomic Networking, Cognitive Networking and Self-Management: In the proceedings of the 5th IEEE MENS Workshop at IEEE Globecom 2013, December." Atlanta, Georgia, USA.
[34] ETSI GS AFI 002: Autonomic network engineering for the self-managing Future Internet (AFI): GANA Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management.This ETSI Specification is publicly available since April 2013: http://www.etsi.org/deliver/etsi_gs/AFI/001_099/002/01.01.01_60/gs_afi002v010101p.pdf
[35] “Autonomic Networking Integrated Model and Approach”, ANIMA, [Online]. Available: https://datatracker.ietf.org/wg/anima/documents/
[36] Santos, José Pedro, et al. "SELFNET Framework self‐healing capabilities for 5G mobile networks." Transactions on Emerging Telecommunications Technologies 27.9 (2016): 1225-1232.
[37] SELFNET Deliverable 2.2 - Definition of APIs and Interfaces for the SELFNET Framework. Main Editors: Pedro Neves, Rui Calé, Altice Labs. Available at https://selfnet-5g.eu/dissemination/
[38] ESTI MEC, [online], available at http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing
[39] ESTI NFV ISG, [online] available at http://www.etsi.org/technologies-clusters/technologies/nfv
[40] Rocks Cluster, [online], available at http://www.rocksclusters.org/wordpress/
[41] HP Insight Cluster Management Utility, [online], available at http://www8.hp.com/us/en/products/server-software/product-detail.html?oid=3296361
[42] MaaS , [online], available at http://www.ubuntu.com/cloud/maas
[43] ONF SDN definition, [online], available at https://www.opennetworking.org/sdn-resources/sdn-definition
[44] Open vSwitch, [online], available at http://openvswitch.org/
[45] SDN, NFV, and Network Virtualization Open Source Projects Directory, https://www.sdxcentral.com/directory/nfv-sdn/open-source-projects/

[46] ONF Real Time Media NBI REST Specification, TR-517, Version 1, Mar 2015, [online], available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Real_Time_Media_NBI_REST_Specification.pdf
[47] Puppet, [online], available at https://puppet.com/
[48] CHEF, [online], available at https://www.chef.io/solutions/configuration-management/
[49] Ansible, [online], available at https://www.ansible.com/
[50] Juju, [online], available at http://www.ubuntu.com/cloud/juju
[51] OpenNMS, [online], available at http://www.opennms.org/
[52] Nagios, [online[, available at https://www.nagios.org/
[53] Ganglia, [online], available at http://ganglia.info/
[54] Zabbix, [online], availalbe at http://www.zabbix.com/

Pedro Neves received his M.S. and PhD degrees in Electronics and Telecommunications Engineering from the University of Aveiro, Portugal, in 2006 and 2012 respectively. From 2003 to 2006 he joined the Telecommunications Institute (IT), Portugal, and participated in the DAIDALOS-I and DAIDALOS-II European funded projects. In 2006 he joined Portugal Telecom Inovação, Portugal, and participated in several European funded projects (e.g. HURRICANE, MEDIEVAL, Cloud4SOA, MCN, CoherentPaaS and T-NOVA). He has been involved in six book chapters, as well as more than 30 scientific papers in major journals and international conferences. His research interests are focused on the integration of the NFV, SDN and SFC (Service Function Chaining) paradigms on the telcos ecosystem.

Rui Calé received his BSc hons (1990) and Master (1997) degrees in Electronics and Telecommunications from the University of Aveiro, Portugal. In 2013 he also received a postgraduate diploma in Information Systems from the Technical University of Lisbon, Portugal. In 1990 Rui joined CET, later PT Inovação, and at present Altice Labs.
In the last 15 years, Rui participated in a large number of development and deployment projects for telecom operators, mostly related with Online Charging and Service Control for fixed and mobile networks throughout the world, both as manager and consultant. From 2010 to present date, as a member of the company's architecture team and an expert in control of Next Generation Networks, worked as a consultant in devising convergence solutions and in promoting SDN and NFV inside the organization.

Mário Rui Costa is the Head of Solutions Architecture & Innovation in Altice Labs, the RD&I Labs of the Altice Telecommunications Group. He is a experienced leader with 20 years experience in the telecommunications industry and more than 5 years experience as Innovation Strategist. For the last 10 years he has been leading Solution Architecture Teams in the communications industry, in different environments, positions and cultures, including national and multinational companies. Mário Rui Costa has strong know-how on BSS, OSS and Network Architectures. His current focal points are Networks Evolution towards SDN, NFV and IoT, explored mainly through the specification of complete solutions and the implementation of internal Proof-Of-Concepts and Field Trials. He is the TM Forum evangelist in Altice Labs.

Gonçalo Nuno Gaspar was born in Covilhã, Portugal, in October 1983. He received the Electronics and Telecommunication Engineering degree from the University of Aveiro, Portugal, in 2006. He joined the Mediation and Activation team from the OSS department at PT Inovação in September 2008. Since then he has developed provisioning and diagnostic solutions for network operators, he is also responsible for the development of the Event and Device Management components of the Network Activator product. Currently he is dedicated to the study of NFV and SDN so that the Network Activator product can evolve and support them.

Prof. Jose M. Alcaraz Calero, SMIEEE, BSc, MEng, PhD is Professor in Networks and Security at University of the West of Scotland. Prof. Alcaraz-Calero has published more than 100 contributions, including 15 patents and intellectual property rights, in international conferences and renowned journals in the fields of network management, management of large-scale data centre and security, his main areas of interest. He has been involved in more than 25 projects totalling more than 20M EUR. Currently, Prof. Alcaraz is Co-Technical Leader of the H2020 SELFNET project, investigating novel automation techniques to achieving advanced self-organized behaviour in complex network management operations. He is member of the NATO IST-118 working group investigating disadvantaged network conditions in the tactical domains.

Qi Wang is a Professor in Networks and Video Communications with the University of the West of Scotland (UWS), UK. He is the Technical Co-Manager of EU Horizon 2020 5G-PPP project SELFNET and Principal Investigator of UK EPSRC project "Enabler for Next-Generation Mobile Video Applications" and a number of other funded projects. His primary research interests include video networking/processing and 5G mobile networks. He has published about 100 peer-reviewed papers and is a winner of several Best Paper Awards from flagship international conferences. He is the Director of Studies for over 10 PhD students and has successfully gradated 4 PhD students in UK. He received his PhD degree in Mobile Networking from the University of Plymouth, UK, with an England ORS Award.

James Nightingale is a Postdoctoral Research Fellow with the University of the West of Scotland (UWS), UK, working on the EU Horizon 2020 5G-PPP project SELFNET. His research interests include mobile networks, multihoming and video streaming techniques. He received the BSc (Honours) degree in Computer Networks from UWS with First Class Honours and won the Best Honours Dissertation Prize. He received his PhD from UWS with Outstanding Progression Award.

Giacomo Bernini received the Italian Laurea degree in Telecommunication Engineering from the University of Pisa, Italy, in 2006. Currently he is R&D Project Manager at Nextworks, and his research interests include SDN and NFV for 5G networks, Cloud Computing, NSI, ASON/GMPLS control plane and PCE frameworks. He participated to design, development and demonstration activities in several FP6, FP7 and H2020 projects as well as to industrial projects. He is currently active in the H2020 5G-PPP Selfnet and ORCHESTRA projects.

Gino Carrozzo holds an Italian Laurea degree "cum laude" in Electronic Engineering and a Ph.D. in Telecommunications Networks, both from the University of Pisa. At Nextworks, Gino is Deputy Head of R&D and Senior Network Architect. He is directly contributing to the R&D strategies and implementations in the SDN/NFV and IoT area. His research activities are currently focused on SDN/NFV for 5G networks, IoT and virtualization. Gino leads and participates in many research projects in Nextworks, with direct experience of various EC funding programs (FP5, FP6, FP7, H2020).

Ángel Leonardo Valdivieso Caraguay was born in Loja, Ecuador, in 1985. He received a B.S. degree in Electronics and Telecommunications Engineering from the Escuela Politécnica Nacional, Quito, Ecuador in 2009 and a M.S. degree in Information Technology from the University of Applied Sciences Hochschule Mannheim, Germany in 2012. He is currently a Ph.D. Student of Computer Engineering in Universidad Complutense de Madrid, Spain. His research interests include computer networks, software-defined networking and network function virtualization.

Luis Javier García Villalba received a Telecommunication Engineering degree from the Universidad de Málaga (Spain) in 1993 and holds a M.Sc. in Computer Networks (1996) and a Ph.D. in Computer Science (1999), both from the Universidad Politécnica de Madrid (Spain). Visiting Scholar at COSIC (Computer Security and Industrial Cryptography, Department of Electrical Engineering, Faculty of Engineering, Katholieke Universiteit Leuven, Belgium) in 2000 and Visiting Scientist at IBM Research Division (IBM Almaden Research Center, San Jose, CA, USA) in 2001 and 2002, he is currently Associate Professor of the Department of Software Engineering and Artificial Intelligence at the Universidad Complutense de Madrid (UCM) and Head of Complutense Research Group GASS, Group of Analysis, Security and Systems (http://gass.ucm.es), which is located in the Faculty of Computer Science and Engineering at the UCM Campus. His professional experience includes projects with Hitachi, IBM, Nokia, Safelayer Secure Communications and H2020. His main research interests are computer security and computer networks (software-defined networks among others).

Anastasius Gavras has more than 20 years of professional experience in academic and industry research. He joined Eurescom, the leading organisation for managing collaborative R&D in telecommunications, more than 15 years ago as programme manager, focusing on the areas of management of networks & systems, security and middleware. In these areas he has managed a large number of studies and projects and has served as rapporteur in standardisation among others in OMG and ITU-T. He is author or co-author of several papers and articles. He is a steering board member of the FI-PPP and is actively involved in 5G-PPP and Future Internet Research and Experimentation (FIRE) initiative. He received his Dipl. Ing. in electrical engineering and electronics from the Technical University Berlin.

Maria Barros Weiss, PhD is Programme Manager at Eurescom. She has managed several projects in areas such as network management, smart cities, IoT/M2M, energy-efficiency, machine-learning, human-machine interfaces, speech processing technologies, and is experienced in International collaborations, with Europe, South America and Sub-Sahara Africa. She has a Ph.D. in Communication and Language technologies from the University of Bonn, Germany; a M.Sc. degree in Computers and Electrical Engineering from the University of Porto, Portugal; and a B.Sc. degree in Computers and Systems Engineering from the

University of Algarve, Portugal. She is the project manager of the H2020 project SELFNET – Framework for Self-organized Network Management in Virtualized and Software Defined Networks project (https://selfnet-5g.eu/).

José Santos is a R&D Engineer at PROEF Group. He has been involved in Innovation projects and EU-funded projects (5G-PPP-SELFNET). He has a M.Sc. degree in Electrical and Computers Engineering from the University of Porto, Portugal; He has a very considerable knowledge of Computer Networks, Mobile Communications and Telecommunication systems. Before joining PROEF group, he was a research intern at INESC TEC in the Wireless Communications Networks (WiN) group.

Ricardo Maia is an Innovation and Development Technician at PROEF. He has been involved in Innovation projects and EU-funded projects (5G-PPP-SELFNET). He has a Sc. Degree from University Fernando Pessoa and two Post-Graduations in Applications Engineer and Computer Graphics from University of Minho. He has a very considerable knowledge of Cloud Computing, Data Center Virtualization and Computer Networks. Before joining PROEF group, he was an IT Engineer at Portugal Telecom in the Cloud and Data Center Area with responsibilities such as the designing and implementing virtualization solutions, testing new products for the data center and managing cloud video surveillance solutions.

Ricardo Preto, Project Manager and Researcher. Since he joined Ubiwhere, he has led and developed multiple QREN and FP7 funded projects. He designed, specified and implemented real-time collaboration solutions (COOLLAB, Eduwall) as well as energy management and optimization decision support systems (SAID-ELD, Enersip) being responsible for both frontend and backend components. In the past three years, he embraced the role of Project Manager of both QREN, in-house and client projects. He led the development of solution such as ANACOM DVB-T (DVBT monitoring solution), uMeter QoS (Internet QoS monitoring solution) or AIBILI (clinical trials centralized solution). Recently, Ricardo joined the TELCO research team contributing to Ubiwhere's R&D activities on areas such as NFV and SDN. He has assumed the role of Project Manager and Researcher of Ubiwhere's activities on two 5G-PP projects (SONATA and SELFNET).

Highlights

- Autonomic network management framework to achieve self-organizing capabilities
- Machine-based, human-assisted network management paradigm
- Leverage on NFV, SDN, SON and Cloud Computing standards & interfaces